

Thales TCT Solutions for CISA Zero Trust Maturity Model 2.0



Contents

Zero Trust - What is it? 3

Implicit Trust - The Problem with Perimeters 3

CISA Zero Trust Maturity Model..... 3

Thales TCT Solutions for Zero Trust 4

Pillar 1: Identity (Section 5.1)..... 4

Pillar 2: Devices (Section 5.2) 5

Pillar 3: Networks (Section 5.3) 5

Pillar 4: Applications & Workloads (Section 5.4) 6

Pillar 5: Data (5.5)..... 8

Cross-Cutting Capabilities (5.6)..... 9

Thales TCT Solutions Address CISA Zero Trust Architecture Pillars 10

Thales TCT Zero Trust Solutions Product Mapping 16

Steps for Zero Trust Architecture Improvements..... 19

About Thales Trusted Cyber Technologies 19

Zero Trust - What is it?

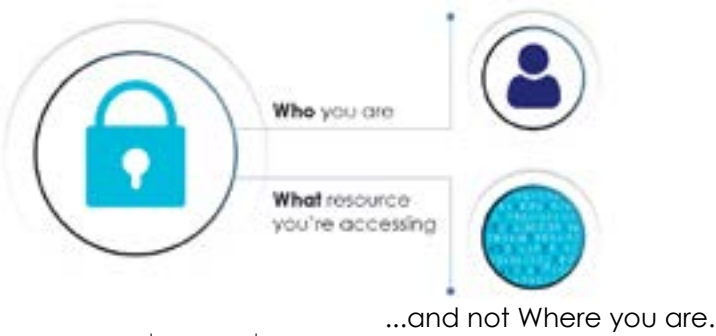
As defined by the National Institute of Standards and Technology (NIST) 800-207, “Zero Trust is the term for an evolving set of cybersecurity paradigms that move defenses from static, network based perimeters to focus on users, assets, and resources.” In order to establish Zero Trust guidelines, NIST and the Cybersecurity and Infrastructure Security Agency (CISA) examined how federal networks were being protected and how data and assets within those networks were protected across the industry. NIST and CISA concluded that most agencies heavily dependent on their perimeter-based defenses, like firewalls, VPNs, in order to control initial access to networks. However, once users gained access to the network, their activities were not well monitored or well tracked. Traditional perimeter security measures generally consider all users trusted once inside a network—including threat actors and malicious insiders. Zero Trust helps agencies prevent data breaches and protect assets by assuming no entity is trusted inside or outside the network. Zero Trust recognizes that when it comes to security, trust is a vulnerability.

Implicit Trust - The Problem with Perimeters

Digital transformation has greatly expanded agencies’ network perimeters. As agencies begin to offer additional services throughout the network—like cloud storage, SaaS applications, remote access to data and resource, etc.—the perimeter of trust is expanded. When data and users who need access to it move outside the traditional perimeter, maintaining access, control, and protection of data becomes even more difficult. Reliance on perimeter security is no longer effective.

Never Trust —Always Verify

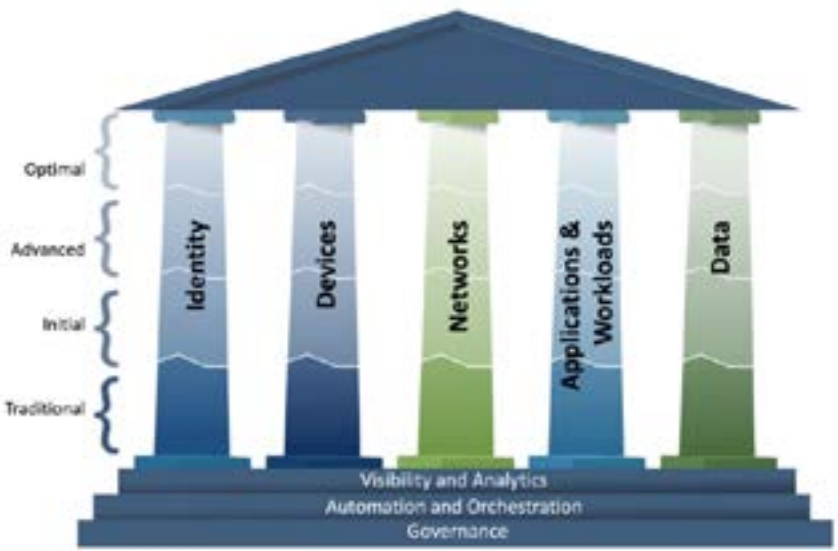
When applications are delivered from the core to the cloud to the edge, where users are located everywhere and where multiple devices are in use, the ability to rely on a single point of trust is untenable. All interactions are inherently risky, necessitating a “never trust, always verify” stance. By default, all transactions within an organization are should be considered untrusted (default deny access) and access/transactions should be based on who the user or entity is and what resource they are accessing—eliminating the outdated requirement for location-based access control (i.e. outside or within the network perimeter)



CISA Zero Trust Maturity Model

The Cybersecurity & Infrastructure Security Agency (CISA) released its [Zero Trust Maturity Model Version 2.0](#) in April 2023. CISA states that “the maturity model, which includes five pillars and three cross-cutting capabilities, is based on the foundations of Zero Trust. Within each pillar, the maturity model provides specific measures required to achieve traditional, initial, advanced, and optimal Zero Trust Architectures.” The latest version of CISA’s Zero Trust Maturity Model better aligns with the Office of Management and Budget (OMB) Memo M-22-09, which outlines the Federal Government’s Zero Trust Architecture strategy and requires agencies to meet specific objectives by the end of Fiscal Year 2024.

CISA’s Zero Trust Maturity Model is broken into five foundational pillars of Zero Trust: Identity, Devices, Networks, Applications & Workloads, and Data. Each pillar contains requirements that align to levels of maturity (traditional, initial, advanced, optimal).



Source: CISA Zero Trust Maturity Model - Zero Trust Maturity Evolution

Thales TCT Solutions for Zero Trust

Thales Trusted Cyber Technologies (TCT) is a U.S. based provider of government high-assurance data security solutions. Thales TCT offers authentication, encryption, and key management solutions that align to CISA's Zero Trust Maturity Model and address the foundational pillars of Zero Trust: Identity, Devices, Networks, Applications & Workloads, and Data.

Pillar 1: Identity (Section 5.1)

Identities are the cornerstone of a Zero Trust Architecture (ZTA). CISA Zero Trust Maturity Model defines identities as an attribute or set of attributes that uniquely describe an agency user or entity, including non-person entities. Agencies should ensure and enforce user and entity access to the right resources at the right time for the right purpose without granting excessive access.

The maturity model states that agencies should ensure and enforce user and entity access to the right resources at the right time for the right purpose without granting excessive access. Agencies should integrate identity, credential, and access management solutions where possible throughout their enterprise to enforce strong authentication, grant tailored context-based authorization, and assess identity risk for agency users and entities. Agencies should integrate their identity stores and management systems, where appropriate, to enhance awareness of enterprise identities and their associated responsibilities and authorities.

Multi-Factor Authentication

Thales TCT provides an end-to-end access management and authentication platform that meets all the Identity Pillar requirements of the CISA Zero Trust Maturity Model. With the Thales' Identity Platform, agencies get a centralized risk-based access platform which supports a broad range of strong multi-factor authentication (MFA) and risk-based authentication to protect all services, apps and environments whether hosted, on-premises or in the cloud.

Offering the broadest range of authentication methods and form factors, Thales TCT allows Federal agencies to address numerous use cases, including authentication, physical access, digital signature, and encryption. *Thales's Identity Platform* is an enterprise-wide identity system that supports a broad range of authentication methods, including:

- PIV cards
- FIDO2 devices
- Virtual PKI smart card
- PKI smart cards and USB authenticators
- High Assurance smart card and tokens designed for U.S. Government Networks
- Two factor Push OTP in combination with biometric, contextual and risk based authentication
- Two factor OTP hardware authenticators
- Contextual / adaptive authentication
- Risk-based authentication

Phishing-Resistant MFA

Thales TCT provides a large portfolio of phishing-resistant authentication methods including PIV cards, FIDO devices, and certificate-based smart cards and USB tokens. Thales also offers combined PKI and FIDO authentication in a single device enabling organizations to transition to FIDO or maintain both methods as needed.

Access Management

Thales TCT's access management solutions have robust policy engines which allow for setting access policies that are extremely flexible. Security policies cater for the creation of very granular and specific rules to constantly reassess users during an open session, rather than only for certain events such as authentication time-outs. If the level of risk changes, Thales TCT's access management solution forces the user to re-authenticate or step up to a stronger form of authentication. Policies can be set per application, apply to network ranges, operating systems, and user collections and geolocations. Authentication rules can be established as dynamic and as context specific as needed adapting to changes in a dynamic cloud environment.

Non-Person Entity Identity Credentials

Thales TCT's *Luna Credential System (LCS)* introduces a new approach to multi-factor authentication by maintaining user or non-person entities credentials in a centralized hardware device that is securely accessible by endpoints in a distributed network. It unites the familiarity of certificate-based authentication with the security of a FIPS 140 certified hardware security module. LCS is a multi-purpose, secure credential system ideally suited for an environment in which the endpoints cannot use a traditional small form factor token. Ideally suited for Robotic Process Automation (RPA) and fully integrated with industry leading RPA vendors such as UiPath and Blue Prism.

Pillar 2: Devices (Section 5.2)

The integrity of devices connecting to agency networks—whether agency-owned or bring-your-own device (BYOD)—must be validated. Unauthorized devices must be prevented from accessing agency networks and data.

Hardware Security Modules (HSMs)

Whether the solution involves device attestation, trusted platform modules, secure boot, or similar device integrity technologies, there is always a concept of device identity involved. Thales TCT's *Luna T-Series HSMs* are a foundational element in all of these solutions by generating secure device identities or cryptographically signing identity-related data.

Luna Credential System

Thales TCT's *Luna Credential System* enhances device deployments by enabling centralized, securely accessible credentials for non-person entities to enable automation of device compliance, risk management processes, and enforcement mechanisms.

Policy Enforcement & Compliance Monitoring

Thales Imperva Data Security Fabric (DSF) provides database vulnerability assessment capabilities to allow organizations to ensure that databases are configured securely whether they run on hardware, virtual environments, cloud environments or as database as a service. Security checklists such as DISA STIGs or Center for Internet Security (CIS) benchmarks for databases are included as prepackaged scan policies as well as dozens of Imperva's custom database vulnerability scan policies. Vulnerability assessments can be configured to execute automatically on a schedule and outputs can be displayed in detailed reports and dashboards. Scan results can also be integrated with ticketing systems to further an organization's ability to manage and effectively remediate findings.

Pillar 3: Networks (Section 5.3)

CISA ZTAs "enable a shift away from traditional perimeter-focused approaches to security and permit agencies to manage internal and external traffic flows, isolate hosts, enforce encryption, segment activity, and enhance enterprise-wide network visibility."

Network Encryption

Thales TCT's *High Speed Encryption (HSE)* solutions offer high-assurance encryption through secure, dedicated encryption devices that feature embedded, zero-touch encryption key management, end-to-end, authenticated encryption and use standards-based algorithms. Thales HSEs are available as a virtual appliance or a hardware-based, stand-alone appliances ranging in performance from 100 Mb to 100 Gb. Thales HSEs are suited for environments including:

- Big Data Applications
- Data Center Interconnect
- 'Mega Data' Campus Network Environments
- Cloud Computing Services 'Backbones'
- Aggregating High-Speed Network Links
- Large Scale, MAN and WAN Security



Thales HSE Features:

- **Certified Security.** Thales HSEs are FIPS 140-2 L3, Common Criteria, NATO, DoD Information Network Approved Products List (DoDIN APL) certified. Our solutions support standards-based, end-to-end authenticated encryption and client-side key management. Advanced security features include traffic flow security, support for a wide range of elliptic curves (Safe Curves, Brainpool, NIST). VLAN based encryption provides unique key pairs in hub and spoke environments to protect against mis-configured traffic. For high-assurance environments, the encryptors also support nested encryption.
- **Transport Independent Mode.** Transforming the network encryption market, Thales HSEs are the first to offer Transport Independent Mode (TIM) network layer independent (covering OSI Layer 2, Layer 3, and Layer 4) and protocol agnostic data in motion encryption.
- **Fully Interoperable.** A single platform can be used to centrally manage encryptors across either single links or distributed networks.
- **Crypto-Agility.** Thales HSE Solutions are crypto-agile, meaning they support customizable encryption for a wide range of elliptic and custom curves support. Thales HSEs already leverage Quantum Key Distribution (QKD) and Quantum Random Number Generation (QRNG) capabilities for future-proofing data security.

Hardware Security Modules

Thales TCT's **Luna T-Series HSMs** protect SSL/TLS sessions, a keystone protocol of data-in-motion security, by generating and storing private keys in a high-assurance, hardware root of trust. Thales HSMs are also crypto-agile, capable of supporting a wide range of encryption standards and updated regularly to ensure the hardware deployed today meets the encryption challenges of tomorrow.

Pillar 4: Applications & Workloads (Section 5.4)

CISA states that agencies should manage and secure their deployed applications and should ensure secure application delivery. Granular access controls and integrated threat protections can offer enhanced situational awareness and mitigate application-specific threats. Per OMB M-22-09, agencies should begin to explore opportunities to make their applications available over public networks to authorized users. Best practices for DevSecOps and CI/CD processes, including the use of immutable workloads, should also be adopted to the extent possible. 30,31 Agencies should explore options to shift their operations away from a focus on accreditation boundaries and updating ATOs to supporting applications as if they are externally facing and provide commensurate security.

Access Management Solutions

Thales TCT's **access management solutions** protect applications and the data behind them by ensuring the right user has access to the right resource at the right level of trust. Agencies can control access by setting granular policies so authorized individuals can do their jobs efficiently and effectively. Agencies can monitor user access permissions and the risks associated with each login, applying step-up authentication only when the user's context changes and the level of risk is concerning.

Application Security

Imperva Application Security empowers agencies to protect their applications and mitigate risk while providing an optimal user experience. Imperva deploys an integrated defense-in-depth model which provides a layered approach to enforcing security from the application to the end user. Through Imperva Runtime Application Self-Protection (RASP), a lightweight agent is incorporated during the software development cycle.

Imperva provides **Web Application Firewall** (WAF) solution (on-premises or virtual appliance WAF Gateway) to defend against all OWASP Top 10 threats including SQL injection, cross-site scripting, illegal resource access, and remote file inclusion. Inspection and enforcement of user traffic occurs across Imperva's global network of PoPs, each also a DDoS scrubbing center. Policies and signatures are kept up-to-date for your WAF and **API Security** based on live, crowd sourced intelligence and from security experts at Imperva Research Labs. Imperva API Security provides continuous protection of all APIs using deep discovery and classification to detect all public, private and shadow APIs. It also protects against business logic attacks and many more of the OWASP API Top Ten. The easy-to-deploy solution empowers security teams to implement a positive API security model.

Imperva **Attack Analytics**, a key part of Imperva Application Security, combats alert fatigue by distilling millions of security alerts into a prioritized set of security insights. It gives recommended actions to improve your security posture, helping you recognize your cyber risk and help bring it down.

Imperva Application Security provides powerful **DDoS Protection** and **Advanced Bot Protection** to eliminate attacks long before malicious traffic even has a chance to reach a website. Multiple DDoS protection services are available, with always-on protection for websites, DNS servers, and individual IPs, and always-on or on-demand protection for networks. With near-zero latency and backed by a 3-second service level agreement for network protection, DDoS traffic is mitigated without disruption to legitimate traffic. And with Imperva Advanced Bot Protection, fingerprinting and client classification categorizes whether traffic is coming from a human, a good bot or a bad bot. It does so quickly and accurately, with a very low false positive rate, protecting websites, mobile apps and APIs against all OWASP 21 automated threats, including account takeover, web scraping, business logic abuse and fraud.

Client-side protection further helps organizations secure every aspect of their web applications and ensure the safety and privacy of their data. It mitigates the risk of client-side attacks that exfiltrate sensitive data, resulting in devastating, costly data breaches. By providing clear visibility with actionable insights and easy controls, Imperva empowers your security team to effortlessly determine the nature of each service and block any unapproved ones.

Imperva Runtime Application Self Protection (RASP) is a NIST SP 800-53 specifically enumerated technology that protects applications “by default”. Imperva RASP protects any application (custom or off-the-shelf) from zero day vulnerabilities in applications written in Java, Node.js, .Net, .Net Core and Python as well as the third party libraries used in their development. Imperva RASP is a signatureless solution that can work in air gapped environments, requires no code changes and can be integrated into an organizations CI/CD pipeline, allowing DEVSECOPS teams to effectively “bake in” security to each software release. Imperva RASP follows the application wherever it runs – on prem, cloud services platforms, containerized environments and even serverless environments.

Data Protection & Key Management

CipherTrust Data Security Platform (CDSP) is an integrated suite of data-centric security solutions that unifies data discovery and classification, data protection, and provides unprecedented granular access controls, all with centralized key management. In addition to providing a data-centric security solution as detailed later in this document, CDSP also integrates with agency workloads to provide authentication, access control, and visibility.

Application Data Protection for DevSecOps

CISA also recommends that agencies apply Zero Trust principles to the development and deployment of applications.

CipherTrust Application Data Protection supports the rapidly evolving needs of DevOps and DevSecOps, targeting the desired combination of rapid software evolution with security. It offers simple-to-use, powerful software tools for application-level key management and encryption of sensitive data. The solution is flexible enough to encrypt nearly any type of data passing through an application. Application-layer data protection can provide the highest level of security, as it can take place immediately upon data creation or first processing and can remain encrypted regardless of its data life cycle state – during transfer, use, backup or copy.

CipherTrust Application Data Protection can be deployed in physical, private or public cloud infrastructure to secure data even when it is migrating from one environment to another, without any modifications to existing encryption or data processing policies.

CipherTrust Application Data Protection is deployed with ***CipherTrust Manager***, an architecture that centralizes key and policy management across multiple applications, environments, or sites. The combined solution provides granular access controls that separate administrative duties from data and encryption key access. For example, a policy can be applied to ensure that no single administrator can make a critical configuration change without additional approval.

Hardware Security Modules

Luna T-Series HSMs secure application development by providing a secure, hardware-based key for signing of software code. Able to be configured to require multi-party, multi-factor authentication to complete a code signing request, Luna T-Series HSMs can provide high assurance that an application has not been maliciously altered prior to deployment. And as a CNSS approved HSM, Luna T-Series HSMs are capable of providing hardware security for LMS code signing keys in accordance with CNSA 2.0.



Pillar 5: Data (5.5)

CISA defines data as “all structured and unstructured files and fragments that reside or have resided in federal systems, devices, networks, applications, databases, infrastructure, and backups (including on-premises and virtual environments) as well as the associated metadata.” The CISA Zero Trust Maturity models states that agency data should be protected on devices, in applications, and on networks in accordance with federal requirements. Agencies should inventory, categorize, and label data; 33 protect data at rest and in transit; and deploy mechanisms to detect and stop data exfiltration. Agencies should carefully craft and review data governance policies to ensure all data lifecycle security aspects are appropriately enforced across the enterprise.

Taking a data-centric approach to security is not only a core component of ZTA, but it also critical for any cybersecurity infrastructure.

Data Discovery & Classification

Data Discovery & Classification (DDC) automatically discovers all data stores in your data estate—from structured to semi-structured to unstructured—across on-premises, hybrid, cloud, and multicloud environments. Automated discovery and classification is the only reliable way to routinely and consistently discover and classify new or modified data stores as your data estate grows and expands—eliminating error-prone and costly manual procedures in the process. DDC can programmatically identify and classify all sensitive data across your data estate, pinpointing its location and providing a risk-based prioritization to each asset that can help organizations plan their risk mitigation programs, systems, and policies.

Data-at-Rest Encryption

CipherTrust Data Security Platform (CDSP) is an integrated suite of data-centric security solutions that unifies data discovery and classification, data protection, and provides unprecedented granular access controls, all with centralized key management.

CipherTrust Transparent Encryption delivers data-at-rest encryption, privileged user access controls and detailed data access audit logging. Agents protect data in files, volumes and databases on Windows, AIX and Linux OS's across physical and virtual servers in cloud and big data environments. Security intelligence logs and reports streamline compliance reporting and speed up threat detection using leading security information and event management (SIEM) systems.

CipherTrust Application Data Protection delivers crypto functions such as key management, signing, hashing and encryption services through APIs, so that developers can easily secure data at the application server or big data node. The solution comes with supported sample code so that developers can move quickly to securing data processed in their applications. CipherTrust Application Data Protection accelerates development of customized data security solutions, while removing the complexity of key management from developer responsibility and control. In addition, it enforces strong separation of duties through key management policies that are managed only by security operations.

CipherTrust Tokenization is offered both vaulted and vaultless and can help reduce the cost and complexity of complying with data security mandates such as PCI-DSS. Tokenization replaces sensitive data with a representative token, so that the sensitive data is kept separate and secure from the database and unauthorized users and systems. The vaultless offering includes policy-based dynamic data masking. Both offerings make it easy to add tokenization to applications.

CipherTrust Database Protection solutions integrate data encryption for sensitive fields in databases with secure, centralized key management and without the need to alter database applications. CipherTrust Database Protection solutions support Oracle, Microsoft SQL Server, IBM DB2 and Teradata databases.

CipherTrust Manager is the central management point for the platform. It is an industry-leading enterprise key management solution that enables organizations to centrally manage encryption keys, provide granular access controls and configure security policies. CipherTrust Manager manages key lifecycle tasks including generation, rotation, destruction, import and export, provides role based access control to keys and policies, supports robust auditing and reporting, and offers development- and management-friendly REST APIs.

Luna T-Series HSMs are the choice for government agencies when storing, protecting and managing cryptographic keys used to secure sensitive data and critical applications. Meeting government mandates for U.S. Supply Chain, the high-assurance, tamper-resistant Luna T-Series HSMs are designed, developed, manufactured, sold, and supported in the United States. Luna T-Series models offer secure storage of your cryptographic information in a controlled and highly secure environment. All Luna T-Series models can be initialized by the customer to protect proprietary information by using either multifactor (PED) authentication or password authentication.



Data Activity Monitoring

Imperva Database Security Fabric (DSF) provides continuous monitoring to capture and analyze all data store activity from both application and privileged user accounts, providing detailed audit trails that show the who, what, when, from where, and the effects of such access (query, modification, deletion) as well as the appropriateness of such access. It unifies auditing across diverse on-premises platforms, providing oversight for relational databases, NoSQL databases, mainframes, big data platforms, and data warehouses. It also supports databases hosted in Microsoft Azure and Amazon Web Services (AWS) — including PaaS offerings such as Azure SQL and Amazon Relational Database Services (RDS). Detailed data activity is captured automatically, making it easier to fulfill compliance requirements as well as provided the detailed insights to take immediate action.

Risk Analytics & Insights

Imperva *Data Risk Analytics (CRA) and Insights* uses automation and machine learning to detect unusual/potentially improper data access and risky behavior from billions of data access activities that occur daily within an organization's data stores (structured, semi-structured and unstructured). It automatically learns the normal behavior of the users -- what they typically access, and how they use such data. DRA then produces actionable insights (provided in detailed narrative form) of potentially dangerous data access that can be investigated immediately and entered into a SOAR workflow system for incident response.

Cross-Cutting Capabilities (5.6)

The cross-cutting capabilities of Visibility and Analytics, Automation and Orchestration, and Governance can be applied across all five Zero Trust pillars. CISA defines Visibility and Analytics as support for comprehensive visibility that informs policy decisions and facilitates response activities. Automation and Orchestration capabilities then leverage these insights to support robust and streamlined operations to handle security incidents and respond to events as they arise. And, Governance enables agencies to manage and monitor their regulatory, legal, environmental, federal, and operational requirements in support of risk-based decision making. Governance capabilities also ensure the right people, process, and technology are in place to support mission, risk, and compliance objectives.

Data Visibility & Analytics

Imperva Data Security Fabric (DSF) and Data Risk Analytics (DRA) provide advanced anomaly base User Entity Based Analytics (UEBA) to detect unusual data access. Taking data access audit data, DSF and DRA can automatically generate actionable insights that allow security practitioners to take immediate remedial action.

Automation & Orchestration Capability

Imperva Data Security Fabric (DSF) integrates with third party systems (such as ticketing systems and security event incident manager (SEIM)) to enable a cyber security information to automate and effectively manage all suspicious data access events.

Thales TCT Solutions Address CISA Zero Trust Architecture Pillars

Pillar	Function	Traditional	Initial	Advanced	Optimal
Identity	Authentication	Agency authenticates identity using either passwords or multi-factor authentication ²¹ (MFA) with static access for entity identity.	Agency authenticates identity using MFA, which may include passwords as one factor and requires validation of multiple entity attributes (e.g., locale or activity)	Agency begins to authenticate all identity using phishing-resistant MFA and attributes, including initial implementation of password less MFA via FIDO2 or PIV23.	Agency continuously validates identity with phishing-resistant MFA, not just when access is initially granted.
	Identity Stores	Agency only uses self managed, on-premises (i.e., planned, deployed, and maintained by agency) identity stores.	Agency has a combination of self-managed identity stores and hosted identity store(s) (e.g., cloud or other agency) with minimal integration between the store(s) (e.g., Single Sign on.)	Agency begins to securely consolidate and integrate some self-managed and hosted identity stores.	Agency securely integrates their identity stores across all partners and environments as appropriate.
	Risk Assessments	Agency makes limited determinations for identity risk (i.e., likelihood that an identity is compromised)	Agency determines identity risk using manual methods and static rules to support visibility.	Agency determines identity risk with some automated analysis and dynamic rules to inform access decisions and response activities.	Agency determines identity risk in real time based on continuous analysis and dynamic rules to deliver ongoing protection.
	Access Management	Agency authorizes permanent access with periodic review for both privileged and unprivileged accounts.	Agency authorizes access, including for privileged access requests, that expires with automated review.	Agency authorizes need based and session-based access, including for privileged access request, that is tailored to actions and resources.	Agency uses automation to authorize just-in-time and just-enough access tailored to individual actions and individual resource needs.
	Visibility & Analytics Capability	Agency collects user and entity activity logs, especially for privileged credentials, and performs some routine manual analysis.	Agency collects user and entity activity logs and performs routine manual analysis and some automated analysis, with limited correlation between log types.	Agency performs automated analysis across some user and entity activity log types and augments collection to address gaps in visibility.	Agency maintains comprehensive visibility and situational awareness across enterprise by performing automated analysis over user activity log types, including behavior-based analytics.
	Automation & Orchestration Capability	Agency manually orchestrates (onboards, offboards, and disables) self-managed identities (users and entities), with little integration, and performs regular review.	Agency manually orchestrates privileged and external identities and automates orchestration of non-privileged users and of self-managed entities.	Agency manually orchestrates privileged user identities and automates orchestration of all identities with integration across all environments.	Agency automates orchestration of all identities with full integration across all environments based on behaviors, enrollments, and deployment needs.
	Governance Capability	Agency implements identity policies (authentication, credentials, access, lifecycle, etc.) with enforcement via static technical mechanisms and manual review.	Agency defines and begins implementing identity policies for enterprise-wide enforcement with minimal automation and manual updates.	Agency implements identity policies for enterprise-wide enforcement with automation and updates policies periodically.	Agency implements and fully automates enterprise wide identity policies for all users and entities across all systems with continuous enforcement and dynamic updates.

PKI Authentication Solutions (Authentication/HSPD 12)

RPA - AI - ML Solutions (Data In Use)

Pillar	Function	Traditional	Initial	Advanced	Optimal
Device	Policy Enforcement & Compliance Monitoring	Agency has limited, if any visibility (i.e., ability to inspect device behavior) into device compliance with few methods of enforcing policies or managing software, configurations, or vulnerabilities.	Agency receives self-reported devices characteristics (eg, keys, tokens, users, etc., on the device) but has limited enforcement mechanisms. Agency has a preliminary, basic process in place to approve software use and push updates and configuration changes to devices.	Agency has verified insights (ie, an administrator can inspect and verify the data on device) on initial access to device and enforces compliance for most devices and virtual assets. Agency uses automated methods to manage devices and virtual assets, approve software, and identify vulnerabilities and install patches.	Agency continuously verifies insights and enforces compliance throughout the lifetime of devices and virtual assets. Agency integrates device, software, configuration, and vulnerability management across all agency environments, including for virtual assets.
	Asset & Supply Chain Risk Management	Agency does not track physical or virtual assets in an enterprise-wide or cross vendor manner and manages its own supply chain acquisition of devices and services in ad hoc fashion with a limited view of enterprise risks.	Agency tracks all physical and some virtual assets and manages supply chain risks by establishing policies and control baselines according to federal recommendations using a robust framework, (e.g., NIST SCRM.) ²⁵	Agency begins to develop a comprehensive enterprise view of physical and virtual assets via automated processes that can function across multiple vendors to verify acquisitions, track development cycles, and provide third-party assessments.	Agency has a comprehensive, at- or near real-time view of all assets across vendors and service providers, automates its supply chain risk management as applicable, builds operations that tolerate supply chain failures, and incorporates best practices.
	Resource Access	Agency does not require visibility into devices or virtual assets used to access resources.	Agency requires some devices or virtual assets to report characteristics then use this information to approve resource access.	Agency's initial resources access considers verified device or virtual asset insights.	Agency's resources access considers real-time risk analytics within devices and virtual assets.
	Device Threat Protection	Agency manually deploys threat protection capabilities to some devices.	Agency has some automated processes for deploying and updating threat protection capabilities to devices and to virtual assets with limited policy enforcement and compliance monitoring integration.	Agency begins to consolidate threat protection capabilities to centralized solutions for devices and virtual assets and integrates most of these capabilities with policy enforcement and compliance monitoring.	Agency has a centralized threat protection security solution(s) deployed with advanced capabilities for all devices and virtual assets and a unified approach for device threat protection, policy enforcement, and compliance monitoring.
	Visibility & Analytics Capability	Agency uses a physically labeled inventory and limited software monitoring to review devices on a regular basis with some manual analysis.	Agency uses digital identifiers (e.g., interface addresses, digital tags) alongside a manual inventory and endpoint monitoring of devices when available. Some agency devices and virtual assets are under automated analysis (e.g., software-based scanning) for anomaly detection based on risk.	Agency automates both inventory collection (including endpoint monitoring on all standard user devices, e.g., desktops and laptops, mobile phones, tablets, and their virtual assets) and anomaly detection to detect unauthorized devices.	Agency automates status collection of all network connected devices and virtual assets while correlating with identities, conducting endpoint monitoring, and performing anomaly detection to inform resource access. Agency tracks patterns of provisioning and/or deprovisioning of virtual assets for anomalies.
	Automation & Orchestration Capability	Agency manually provisions, configures, and/or registers devices within the enterprise.	Agency begins to use tools and scripts to automate the process of provisioning, configuration, registration, and/or deprovisioning for devices and virtual assets.	Agency has implemented monitoring and enforcement mechanisms to identify and manually disconnect or isolate non-compliant (vulnerable, unverified certificate; unregistered mac address) devices and virtual assets.	Agency has fully automated processes for provisioning, registering, monitoring, isolating, remediating, and deprovisioning devices and virtual assets.
	Governance Capability	Agency sets some policies for the lifecycle ²⁶ of their traditional and peripheral computing devices and relies on manual processes to maintain (e.g., update, patch, sanitize) these devices.	Agency sets and enforces policies for the procurement of new devices, the lifecycle of non-traditional computing devices and virtual assets, and for regularly conducting monitoring and scanning of devices	Agency sets enterprise-wide policies for the lifecycle of devices and virtual assets, including their enumeration and accountability, with some automated enforcement mechanisms.	Agency automates policies for the lifecycle of all network-connected devices and virtual assets across the enterprise.

Physical Protections -
Roots of Trust (HSM,
Key Management)

Application
Security/ Analytics
& Insight/Data
Discovery (Imperva)

Pillar	Function	Traditional	Initial	Advanced	Optimal
Network	Network Segmentation	Agency defines their network architecture using large perimeter/macro segmentation with minimal restrictions on reachability within network segments. Agency may also rely on multi-service interconnections (e.g., bulk traffic VPN tunnels).	Agency begins to deploy network architecture with the isolation of critical workloads, constraining connectivity to least function principles, and a transition toward service-specific interconnections.	Agency expands deployment of endpoint and application profile isolation mechanisms to more of their network architecture with ingress/egress micro perimeters and service specific interconnections.	Agency network architecture consists of fully distributed ingress/egress micro perimeters and extensive micro-segmentation based around application profiles with dynamic just-in-time and just-enough connectivity for service-specific interconnections.
	Network Traffic Management	Agency manually implements static network rules and configurations to manage traffic at service provisioning, with limited monitoring capabilities (e.g., application performance monitoring or anomaly detection) and manual audits and reviews of profile changes for mission critical applications.	Agency establishes application profiles with distinct traffic management features and begins to map all applications to these profiles. Agency expands application of static rules to all applications and performs periodic manual audits of application profile assessments.	Agency implements dynamic network rules and configurations for resource optimization that are periodically adapted based upon automated risk-aware and risk-responsive application profile assessments and monitoring.	Agency implements dynamic network rules and configurations that continuously evolve to meet application profile needs and reprioritize applications based on mission criticality, risk, etc.
	Traffic Encryption	Agency encrypts minimal traffic and relies on manual or ad hoc processes to manage and secure encryption keys.	Agency begins to encrypt all traffic to internal applications, to prefer encryption for traffic to external applications ²⁷ , to formalize key management policies, and to secure server/service encryption keys.	Agency ensures encryption for all applicable internal and external traffic protocols, ²⁸ manages issuance and rotation of keys and certificates, and begins to incorporate best practices for cryptographic agility. ²⁹	Agency continues to encrypt traffic as appropriate, enforces least privilege principles for secure key management enterprise wide, and incorporates best practices for cryptographic agility as widely as possible.
	Network Resilience	Agency configures network capabilities on a case-by case basis to only match individual application availability demands with limited resilience mechanisms for workloads not deemed mission critical.	Agency begins to configure network capabilities to manage availability demands for additional applications and expand resilience mechanisms for workloads not deemed mission critical.	Agency has configured network capabilities to dynamically manage the availability demands and resilience mechanisms for the majority of their applications.	Agency integrates holistic delivery and awareness in adapting to changes in availability demands for all workloads and provides proportionate resilience.
	Visibility & Analytics Capability	Agency incorporates limited boundary-focused network monitoring capabilities with minimal analysis to start developing centralized situational awareness.	Agency employs network monitoring capabilities based on known indicators of compromise (including network enumeration) to develop situational awareness in each environment and begins to correlate telemetry across traffic types and environments for analysis and threat hunting activities.	Agency deploys anomaly based network detection capabilities to develop situational awareness across all environments, begins to correlate telemetry from multiple sources for analysis, and incorporates automated processes for robust threat hunting activities.	Agency maintains visibility into communication across all agency networks and environments while enabling enterprise-wide situational awareness and advanced monitoring capabilities that automate telemetry correlation across all detection sources.
	Automation & Orchestration Capability	Agency uses manual processes to manage the configuration and resource lifecycle for agency networks and environments with periodic integration of policy requirements and situational awareness.	Agency begins using automated methods to manage the configuration and resource lifecycle for some agency networks or environments and ensures that all resources have a defined lifetime based on policies and telemetry.	Agency uses automated change management methods (e.g., CI/CD) to manage the configuration and resource lifecycle for all agency networks and environments, responding to and enforcing policies and protections against perceived risks.	Agency networks and environments are defined using infrastructure-as-code managed by automated change management methods, including automated initiation and expiration to align with changing needs.
	Governance Capability	Agency implements static network policies (access, protocols, segmentation, alerts, and remediation) with an approach focused on perimeter protections.	Agency defines and begins to implement policies tailored to individual network segments and resources while also inheriting corporate-wide rules as appropriate.	Agency incorporates automation in implementing tailored policies and facilitates the transition from perimeter-focused protections.	Agency implements enterprise-wide network policies that enable tailored, local controls; dynamic updates; and secure external connections based on application and user workflows.











Pillar	Function	Traditional	Initial	Advanced	Optimal	Application Security/ Analytics & Insight/Data Discovery (Imperva)
Application and Workload	Application Access (formerly Access Authorization)	Agency authorizes access to applications primarily based on local authorization and static attributes.	Agency begins to implement authorizing access capabilities to applications that incorporate contextual information (e.g., identity, device compliance, and/or other attributes) per request with expiration.	Agency automates application access decisions with expanded contextual information and enforced expiration conditions that adhere to least privilege principles.	Agency continuously authorizes application access, incorporating real time risk analytics and factors such as behavior or usage patterns.	
	Application Threat Protections (formerly Threat Protection)	Agency threat protections have minimal integration with application workflows, applying general purpose protections for known threats.	Agency integrates threat protections into mission critical application workflows, applying protections against known threats and some application specific threats.	Agency integrates threat protections into all application workflows, protecting against some application-specific and targeted threats.	Agency integrates advanced threat protections into all application workflows, offering real-time visibility and content-aware protections against sophisticated attacks tailored to applications.	
	Accessible Applications	Agency makes some mission critical applications available only over private networks and protected public network connections (e.g., VPN) with monitoring.	Agency makes some of their applicable mission critical applications available over open public networks to authorized users with need via brokered connections.	Agency makes most of their applicable mission critical applications available over open public network connections to authorized users as needed.	Agency makes all applicable applications available over open public networks to authorized users and devices, where appropriate, as needed.	
	Secure Application Development & Deployment Workflow	Agency has ad hoc development, testing, and production environments with non-robust code deployment mechanisms.	Agency provides infrastructure for development, testing, and production environments (including automation) with formal code deployment mechanisms through CI/CD pipelines and requisite access controls in support of least privilege principles.	Agency uses distinct and coordinated teams for development, security, and operations while removing developer access to production environment for code deployment.	Agency leverages immutable workloads where feasible, only allowing changes to take effect through redeployment, and removes administrator access to deployment environments in favor of automated processes for code deployment.	
	Application Security Testing (formerly Application Security)	Agency performs application security testing prior to deployment, primarily via manual testing methods.	Agency begins to use static and dynamic (i.e., application is executing) testing methods to perform security testing, including manual expert analysis, prior to application deployment.	Agency integrates application security testing into the application development and deployment process, including the use of periodic dynamic testing methods	Agency integrates application security testing throughout the software development lifecycle across the enterprise with routine automated testing of deployed applications.	
	Visibility & Analytics Capability	Agency performs some performance and security monitoring of mission critical applications with limited aggregation and analytics.	Agency begins to automate application profile (e.g., state, health, and performance) and security monitoring for improved log collection, aggregation, and analytics.	Agency automates profile and security monitoring for most applications with heuristics to identify application-specific and enterprise-wide trends and refines processes over time to address gaps in visibility.	Agency performs continuous and dynamic monitoring across all applications to maintain enterprise-wide comprehensive visibility.	
	Automation & Orchestration Capability	Agency manually establishes static application hosting location and access at provisioning with limited maintenance and review.	Agency periodically modifies application configurations (including location and access) to meet relevant security and performance goals.	Agency automates application configurations to respond to operational and environmental changes	Agency automates application configurations to continuously optimize for security and performance.	
	Governance Capability	Agency relies primarily on manual enforcement policies for application access, development, deployment, software asset management, security testing and evaluation (ST&E) at technology insertion, patching, and tracking software dependencies.	Agency begins to automate policy enforcement for application development (including access to development infrastructure), deployment, software asset management, ST&E at technology insertion, patching, and tracking software dependencies based upon mission needs (for example, with Software Bill of Materials).	Agency implements tiered, tailored policies enterprise wide for applications and all aspects of the application development and deployment lifecycles and leverages automation, where possible, to support enforcement.	Agency fully automates policies governing applications development and deployment, including incorporating dynamic updates for applications through the CI/CD pipeline.	



Pillar	Function	Traditional	Initial	Advanced	Optimal
Data	Data Inventory Management	Agency manually identifies and inventories some agency data (e.g., mission critical data).	Agency begins to automate data inventory processes for both on-premises and in cloud environments, covering most agency data, and begins to incorporate protections against data loss.	Agency automates data inventory and tracking enterprise-wide, covering all applicable agency data, with data loss prevention strategies based upon static attributes and/or labels.	Agency continuously inventories all applicable agency data and employs robust data loss prevention strategies that dynamically block suspected data exfiltration.
	Data Categorization	Agency employs limited and ad hoc data categorization capabilities.	Agency begins to implement a data categorization strategy with defined labels and manual enforcement mechanisms.	Agency automates some data categorization and labeling processes in a consistent, tiered, targeted manner with simple, structured formats and regular review.	Agency automates data categorization and labeling enterprise-wide with robust techniques; granular, structured formats; and mechanisms to address all data types.
	Data Availability	Agency primarily makes data available from on-premises data stores with some off-site backups.	Agency makes some data available from redundant, highly available data stores (e.g., cloud) and maintains off-site backups for on premises data.	Agency primarily makes data available from redundant, highly available data stores and ensures access to historical data.	Agency uses dynamic methods to optimize data availability, including historical data, according to user and entity need.
	Data Access	Agency governs user and entity access (e.g., permissions to read, write, copy, grant others access, etc.) to data through static access controls.	Agency begins to deploy automated data access controls that incorporate elements of least privilege across the enterprise.	Agency automates data access controls that consider various attributes such as identity, device risk, application, data category, etc., and are time limited where applicable.	Agency automates dynamic just-in-time and just-enough data access controls enterprise-wide with continuous review of permissions.
	Data Encryption	Agency encrypts minimal agency data at rest and in transit and relies on manual or ad hoc processes to manage and secure encryption keys.	Agency encrypts all data in transit and, where feasible, data at rest (e.g., mission critical data and data stored in external environments) and begins to formalize key management policies and secure encryption keys.	Agency encrypts all data at rest and in transit across the enterprise to the maximum extent possible, begins to incorporate cryptographic agility, and protects encryption keys (i.e., secrets are not hard coded and are rotated on a regular basis).	Agency encrypts data in use where appropriate, enforces least privilege principles for secure key management enterprise-wide, and applies encryption using up-to-date standards and cryptographic agility to the extent possible.
	Visibility & Analytics Capability	Agency has limited visibility into data including location, access, and usage, with analysis consisting primarily of manual processes.	Agency obtains visibility based on data inventory management, categorization, encryption, and access attempts, with some automated analysis and correlation.	Agency maintains data visibility in a more comprehensive, enterprise wide manner with automated analysis and correlation and begins to employ predictive analytics.	Agency has visibility across the full data lifecycle with robust analytics, including predictive analytics, that support comprehensive views of agency data and continuous security posture assessment.
	Automation & Orchestration Capability	Agency implements data lifecycle and security policies (e.g., access, usage, storage, encryption, configurations, protections, backups, categorization, sanitization) through manual, and potentially ad hoc, processes.	Agency uses some automated processes to implement data lifecycle and security policies.	Agency implements data lifecycle and security policies primarily through automated methods for most agency data in a consistent, tiered, targeted manner across the enterprise.	Agency automates, to the maximum extent possible, data lifecycles and security policies for all agency data across the enterprise.
	Governance Capability	Agency relies on ad hoc data governance policies (e.g., for protection, categorization, access, inventorying, storage, recovery, removal, etc.) with manual implementation.	Agency defines high-level data governance policies and relies primarily on manual, segmented implementation.	Agency begins integration of data lifecycle policy enforcement across the enterprise, enabling more unified definitions for data governance policies.	Agency data lifecycle policies are unified to the maximum extent possible and dynamically enforced across the enterprise.










RPA - AI - ML Solutions (Data In Use)
File System - NAS Encryption (Data At Rest/In Use)
Network Encryption (Data in Transit)
Physical Protections - Roots of Trust (HSM, Key Management)
Application Security/ Analytics & Insight/Data Discovery (Imperva)

Pillar	Function	Traditional	Initial	Advanced	Optimal
Cross-Cutting Capabilities	Visibility & Analytics	Agency manually collects limited logs across their enterprise with low fidelity and minimal analysis.	Agency begins to automate the collection and analysis of logs and events for mission critical functions and regularly assesses processes for gaps in visibility.	Agency expands the automated collection of logs and events enterprise-wide (including virtual environments) for centralized analysis that correlates across multiple sources.	Agency maintains comprehensive visibility enterprise-wide via centralized dynamic monitoring and advanced analysis of logs and events.
	Automation & Orchestration	Agency relies on static and manual processes to orchestrate operations and response activities with limited automation.	Agency begins automating orchestration and response activities in support of critical mission functions.	Agency automates orchestration and response activities enterprise-wide, leveraging contextual information from multiple sources to inform decisions.	Agency orchestration and response activities dynamically respond to enterprise-wide changing requirements and environmental changes.
	Governance	Agency implements policies in an ad hoc manner across the enterprise, with policies enforced via manual processes or static technical mechanisms.	Agency defines and begins implementing policies for enterprise-wide enforcement with minimal automation and manual updates.	Agency implements tiered, tailored policies enterprisewide and leverages automation where possible to support enforcement. Access policy decisions incorporate contextual information from multiple sources.	Agency implements and fully automates enterprise-wide policies that enable tailored local controls with continuous enforcement and dynamic updates.

Thales TCT Zero Trust Solutions Product Mapping

<div><div> = Cloud-based or virtual appliance offerings available</div><div> = Multi-cloud support</div></div>	Authentication/ PKI Solution (Auth/HSPD12/ CMS)	Card Management Solution (Authentication/ HSPD12)	Digital Signatures Solutions (Data In Use)	RPA/AI/ML Solutions (Data In Use)	File System/ NAS Encryption (Data At Rest/ In Use)	Network Encryption (Data In Transit)	Database Encryption (Data At Rest)	Post-Quantum Encryption	Physical Protections - Roots of Trust (HSM, Key Management)	Application Security/ Analytics & Insight/Data Discovery (Imperva)
Data Security										
Data In Use Protection										
Luna T-series HSM	☑	☑	☑				☑	☑	☑	
Luna Credential System			☑	☑				☑	☑	
Luna as a Service 	☑	☑	☑				☑	☑	☑	
LCS as a Service 			☑	☑				☑	☑	
Data At Rest Protection (DARE)										
Data Discovery & Classification				☑	☑					☑
CipherTrust Manager 				☑	☑		☑	☑	☑	☑
Basic Connectors (file system/CTE, database/CAKM,...) 				☑	☑		☑			☑
Basic Connector Utilities (LDT) 				☑	☑		☑			☑
Advanced Connectors (SAP, SalesForce, ...) 				☑	☑		☑			☑
CipherTrust Cloud Key Manager (CCKM) 					☑		☑			☑
Data In Transit Protection										
High Speed Encryptors 						☑		☑	☑	
SureDrop Secure File Sharing 						☑				
Votiro Secure File & Email Gateways						☑				

	Authentication/ PKI Solution (Auth/HSPD12/ CMS)	Card Management Solution (Authentication/ HSPD12)	Digital Signatures Solutions (Data In Use)	RPA/AI/ML Solutions (Data In Use)	File System/ NAS Encryption (Data At Rest/ In Use)	Network Encryption (Data In Transit)	Database Encryption (Data At Rest)	Post-Quantum Encryption	Physical Protections - Roots of Trust (HSM, HSE, CM, ...)	Application Security/ Analytics & Insight/Data Discovery (Imperva)
Identity Security										
Authentication										
MFA (phishing resistant)	☑	☑		☑						
Smart Cards (PIV, CAC, FIDO2, Readers)	☑	☑	☑							
Tokens (PIV, CAC, FIDO2, NFC, OTP, Biometric)	☑	☑	☑							
Middleware (SIPR, NIPR, HSPD12)	☑									
Identity Providers (IDP)										
STA (cloud-based, currently non- FedRAMP'd) 	☑									
SAS-PCE (on-premise)	☑									
CIAM (Commercial IAM - C2G, G2G)	☑									
Card/Credential Management System (CMS)										
Intercede MyID (over 5000 credentials)	☑	☑	☑	☑						
Versasec (under 5000 credentials)	☑	☑	☑	☑						
XTec CMS (cloud-based, FedRAMP HIGH) 	☑	☑	☑	☑						

	Authentication/ PKI Solution (Auth/HSPD12/ CMS)	Card Management Solution (Authentication/ HSPD12)	Digital Signatures Solutions (Data In Use)	RPA/AI/ML Solutions (Data In Use)	File System/ NAS Encryption (Data At Rest/ In Use)	Network Encryption (Data In Transit)	Database Encryption (Data At Rest)	Post-Quantum Encryption	Physical Protections - Roots of Trust (HSM, HSE, CM, ...)	Application Security/ Analytics & Insight/ Data Discovery (Imperva)
End-to-End Application & Data Security										
Cloud Web Application and API Protection (WAAP)										
Imperva Web Application Firewall (WAF) 										<input checked="" type="checkbox"/>
Imperva API Management & Governance 										<input checked="" type="checkbox"/>
Imperva API Security 										<input checked="" type="checkbox"/>
Imperva Attack Analytics 										<input checked="" type="checkbox"/>
Imperva DDoS Protection & Application Performance 						<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>
Imperva Advanced Bot Protection 				<input checked="" type="checkbox"/>						<input checked="" type="checkbox"/>
Imperva Serverless Protection 										<input checked="" type="checkbox"/>
Imperva Runtime Protection 										<input checked="" type="checkbox"/>
Imperva Data Discovery & Classification 										<input checked="" type="checkbox"/>

Steps for Zero Trust Architecture Improvements

Keep in mind that Zero Trust is a progression and not a discrete goal. There are many ways to get started with a Zero Trust deployment. Thales TCT recommends that organizations should follow these steps for Zero Trust Architecture Improvements:

1. Read Zero Trust guidance - CISA, DoD, OMB, etc.
2. Identify leadership and team for your organization
3. Prioritize critical applications and data
4. Develop a plan based on prioritized objectives
5. Execute and evolve
 - Achieving Zero Trust is iterative
 - It starts with identities and ends with data
 - Your Zero Trust posture will evolve and improve over time

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., is a trusted, U.S. provider of cybersecurity solutions dedicated to U.S. Government. We protect the government's most vital data from the core to the cloud to the edge with a unified approach to data protection. Our solutions reduce the risks associated with the most critical attack vectors and address the government's most stringent encryption, key management, and access control requirements.

For more information, visit www.thalestct.com





Thales Trusted Cyber Technologies
3465 Box Hill Corporate Center Drive
Suite D
Abingdon, MD 21009
info@thalestct.com

© 2024 SafeNet Assured Technologies, LLC.
6.11.24
www.thalestct.com

