Trusted Cyber Technologies

THALES
Building a future we can all trust

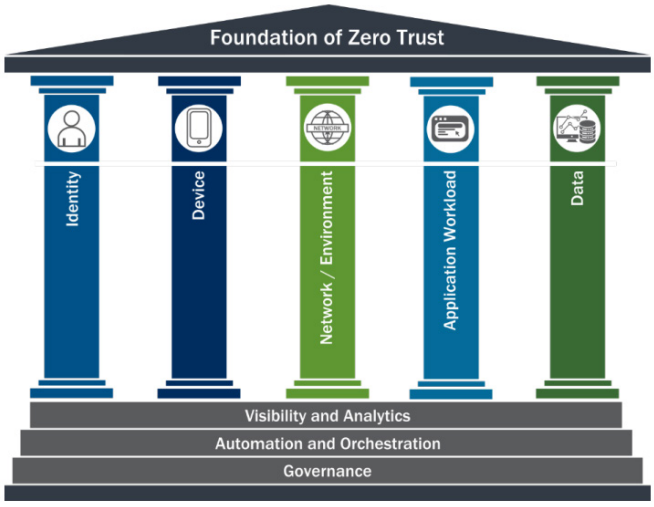
Zero Trust Solutions from Thales Trusted Cyber Technologies

The digital transformation of organizations through the adoption and proliferation of technologies such as IoT, cloud delivery, and mobile adoption have led to the disintegration of the traditional IT security perimeter. In this environment, where applications are delivered from the cloud to the cloud, 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.

What is Zero Trust?

Zero Trust is a strategic initiative and principle that helps organizations prevent data breaches and protect their assets by assuming no entity is trusted. Going beyond the "castle-and-moat" concept which had dominated traditional perimeter security, Zero Trust recognizes that when it comes to security, trust is a vulnerability. Traditional security considered all users trusted once inside a network—including threat actors and malicious insiders.

By eliminating the concept of a "safe" network, Zero Trust requires strict identity verification and moves the decision to authenticate and authorize closer to the resource. The identity of the user/device/service provides key context for the application of access policies. With Zero Trust, access rules are as granular as possible to enforce least privileges required to perform the requested action.



Source: Cybersecurity and Infrastructure Security Agency (CISA)

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 address foundational pillars of Zero Trust: Identity, Device, Network, Application Workload, and Data.

Pillar 1: Identity

Identities are the cornerstone of a Zero Trust Architecture (ZTA). The Cybersecurity & Infrastructure Security Agency (CISA) defines identities as "an attribute or set of attributes that uniquely describe an agency user or entity. Agencies should ensure and enforce that the right users and entities have the right access to the right resources at the right time".[1]

Thales TCT Authentication and Access Management Solutions

From traditional high assurance and commercial-of-the-shelf authentication solutions to first-of-a-kind hardware security module-based identity credentials for non-person entities, Thales TCT offers the most secure, certificate-based authentication platforms available to the U.S. Federal Government supporting the latest and evolving protocols and standards including WebAuth and FIDO.

Thales TCT's wide-range authenticators includes hardware and software OTP tokens, X.509 certificate-based USB tokens and smart cards, OOB, hybrid tokens, and phone tokens for all mobile platforms. Many Thales TCT hardware tokens support physical access control to secure buildings and sites, as well as continuous access online.

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.

Pillar 2: Device

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.

Thales TCT Luna T-Series 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 Luna HSMs are a foundational element in all of these solutions by generating secure device identities or cryptographically signing identity-related data.

Thales TCT Luna Credential System for Non-Person Entity Identity Credentials

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 140-2 certified HSM. 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 3: Network

CISA suggests that "need to align their network segmentation and protections according to the needs of their application workflows instead of the implicit trust inherent in traditional network segmentation"[2] and cites encryption as a key ZTA functionality.

Thales TCT High Speed Encryptors for Network Encryption

Thales' high speed encryption (HSE) solutions offer high-assurance encryption though 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 as available a virtual appliance or as 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.

1, 2 Zero Trust Maturity Model Pre-decisional Draft CISA https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf

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.

Pillar 4: Application Workload

CISA recommends that agencies "integrate their protections more closely with their application workflows to ensure the protections have the visibility and understanding needed to provide effective security".[3]

Thales TCT 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.

Thales TCT CipherTrust Data Security Platform

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.

Thales TCT CipherTrust 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.

Pillar 5: Data

Taking a data-centric approach to security is not only a core component of ZTA, but it also critical for any cybersecurity infrastructure. CISA recommends that "agencies should begin to identify, categorize, and inventory data assets".[4] Next, agencies should deploy security solutions to protect the data itself.

Thales TCT CipherTrust Data Discovery & Classification

CipherTrust Data Discovery & Classification (DDC) locates regulated data, both structured and unstructured, across the cloud, big data, and traditional data stores. A single pane of glass delivers understanding of sensitive data and its risks, enabling better decisions about closing security gaps, compliance violations and prioritizing remediation. DDC provides a streamlined workflow all the way from policy configuration, discovery, and classification, to risk analysis and reporting, helping to eliminate security blind spots and complexities.

Unlike alternative, disjointed solutions that can leave data exposed or compromised, DDC provides a streamlined workflow all the way from policy configuration, discovery, and classification, to risk analysis and reporting. This eliminates security blind spots and complexities. As a result, you can easily uncover and mitigate your data privacy risks, enforce data sovereignty, and proactively respond to a growing number of data privacy and security regulations, including GDPR, CCPA, LGPD, PCI DSS and HIPAA.

Thales TCT 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.

3, 4 Zero Trust Maturity Model Pre-decisional Draft CISA https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf

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 sensitize 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.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled.
For more information, visit www.thalestct.com

3465 Box Hill Corporate Center Drive, Suite D, Abingdon, MD 21009 • 443-484-7070 • info@thalestct.com
thalestct.com