Solution Brief

Thales TCT Zero Trust Solutions

thalestct.com

THALES
Building a future we can all trust

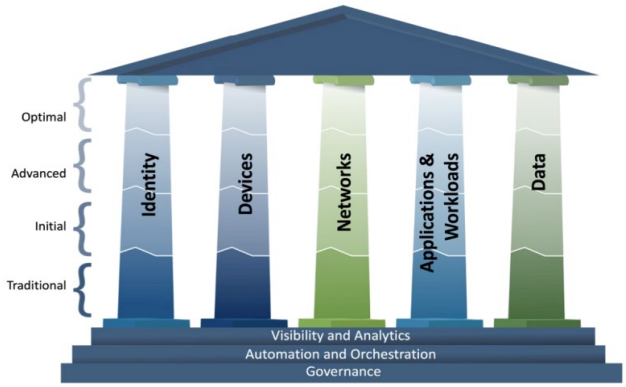
THALES

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: 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 address foundational pillars of Zero Trust: Identity, Devices, Networks, Applications & Workloads, and Data.

Pillar 1: Identity

Identities are the cornerstone of a Zero Trust Architecture (ZTA). Cybersecurity & Infrastructure Security Agency's (CISA) Zero Trust Maturity Model Version 2.0 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."

Identity & Access Management Solutions

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.

- Phishing-resistant MFA including PIV cards, FIDO2 devices. certificate-based smart cards and USB tokens.
- Virtual PKI smart card
- 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

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

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

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.

Luna Credential System

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

CISA indicates the need to "shift away from traditional perimeter-focused approaches to security" and cites data-in-motion encryption as a key ZTA functionality.

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 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. For high-assurance environments, the encryptors also support nested encryption. A single platform can be used to centrally manage encryptors across either single links or distributed networks.

Thales HSEs offer Transport Independent Mode (TIM) network layer independent (covering OSI Layer 2, Layer 3, and Layer 4) and protocol agnostic data in motion encryption.

Thales HSE are crypto-agile and support customizable encryption for a wide range of elliptic and custom curves support. Thales HSEs leverage Quantum Key Distribution (QKD) and Quantum Random Number Generation (QRNG) capabilities for future-proofing data security.

Hardware Security Modules

Thales 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

CISA recommends "granular access controls and integrated threat protections" throughout application development, deployment, and usage.

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's Web Application Firewall (WAF) (on-premises or virtual appliance WAF Gateway) defends 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 10.

Imperva Attack Analytics 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. 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.

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.

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.

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

Taking a data-centric approach to security is not only a core component of ZTA, but it also critical for any cybersecurity infrastructure. CISA notes that data protection extends across an organization's digital infrastructure, "on devices, in applications, and on networks."

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 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.

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 effective manage all suspicious data access events.

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

Contact us - For office location and contact information, please visit thalestct.com/contact-us