thalestct.com

THALES

Thales Trusted Cyber Technologies Product Overview

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

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 most stringent encryption, key management, and access control requirements.

We provide U.S. federal agencies with solutions for their cryptographic infrastructure that have a U.S. supply chain lifecycle. Our core data security solutions are developed, manufactured, sold and supported in the U.S.

We also sell and support industry-leading, third-party commercial-off-the-shelf solutions. We mitigate the risk associated with procuring these data security solutions which are often developed outside of the U.S. As part of the Thales Defense & Security, Inc Defense Counterintelligence and Security Agency (DCSA) proxy, Thales TCT is protected from Foreign Ownership Control and Influence (FOCI). We are also governed by the Committee for Foreign Investment in the U.S. (CFIUS) National Security Agreement established with SafeNet Assured Technologies (Thales TCT's legal entity), which provides further FOCI mitigation to the products and services provided to our customers.

FAST FACTS

U.S. Support | Cleared Employees | U.S. Manufacturing

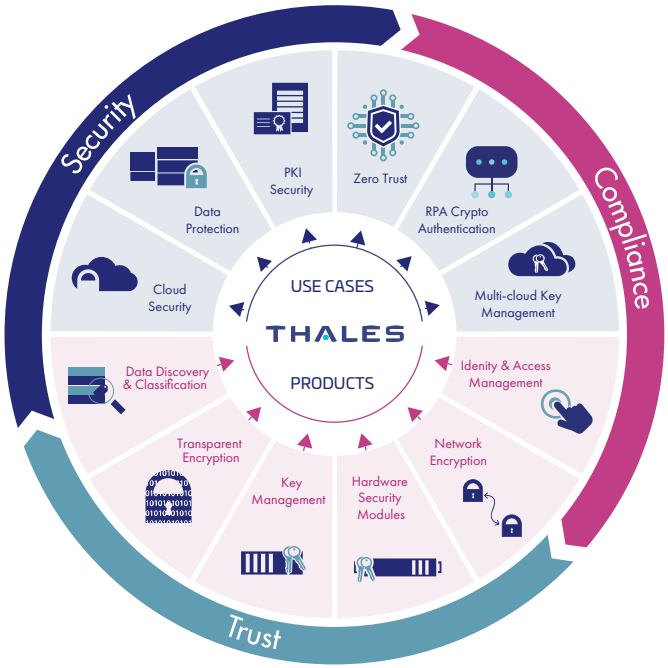
- Headquarters: Abingdon, MD
- Maintain required U.S. Federal Government approvals and certifications to develop, support and sell products to government clients
- Proxy Agreement with Defense Counterintelligence and Security Agency for Foreign Owndership Control and Influence
- National Security Agreement with the Committee on Foreign Investment in the United States
- Trusted U.S. Source of Supply of Key Technologies for the Federal Government
- All of technical and sales support is onshore with only U.S. citizens (fully cleared support Levels 1-3)

Protecting the government's most vital data from the core to the cloud to the edge

Thales TCT offers unified data protection solutions that reduce the risks associated with the most critical attack vectors. Our solutions address government's most pressing cybersecurity challenges such as:

- Zero Trust
- Cloud Security
- Data Protection
- PKI Security
- IdAM Security
- Network Encryption
- Robotic Process Automation
- Quantum
- Ransomware Prevention
- Remote Workforce

Our solutions deliver the same level of security whether deployed in enterprise, cloud, or edge environments. We enable agencies to meet their immediate cybersecurity needs while investing in a solution that provides robust security, a growing ecosystem, and the scalability needed to build a trusted framework for the future.



With Thales TCT's solutions you can:

- **Discover & Classify Data.** Efficiently discover and classify sensitive data, get a clear understanding of data and its risks, and take actions to close the gaps, from a single pane of glass.
- **Encrypt Data-at-Rest.** Protect data with granular encryption and role-based access control for structured and unstructured data residing in databases, applications, files, and storage containers.
- **Protect and Manage Encryption Keys.** Simplify the management of encryption keys across their entire lifecycle, including secure key generation, backup/restore, clustering, deactivation and deletion.
- **Deploy a Secure Root of Trust.** Store, protect and manage crypto keys used to secure sensitive data and critical applications with FIPS 140-2 Level 3 hardware security modules that meets government U.S. supply chain requirements.
- **Protect Data-in-Transit.** Secure sensitive data, real-time video and voice, on the move between data centers and sites with proven high-assurance network security.
- **Control access to sensitive data and protect user identities** Deliver secure, trusted access to all cloud services and enterprise apps using SSO, MFA and robust access policies.

Discover & Classify Data

CipherTrust Data Discovery and Classification
CipherTrust Data Discovery and Classification locates regulated sensitive 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, prioritizing remediation actions, and securing your cloud transformation and third-party data sharing. The solution provides a streamlined workflow from policy configuration, discovery, and classification, to risk analysis and reporting, helping to eliminate security blind spots and complexities.

Encrypt Data-at-Rest | Protect & Manage Encryption Keys

CipherTrust Data Security Platform unifies data discovery, classification, data protection, and unprecedented granular access controls with centralized key management – all on a single platform. This results in less resources dedicated to data security operations, ubiquitous compliance controls, and significantly reduced risk across your agency. The platform includes:

CipherTrust Manager
CipherTrust Manager is the central management point for the platform. It offers an industry-leading enterprise key management solution enabling organizations to centrally manage encryption keys, provide granular access controls and configure security policies. It 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 developer friendly REST APIs. It provides centralized management of encryption keys and policies for its data protection connectors, discussed below. CipherTrust Manager is available in both virtual and physical form-factors that are FIPS 140-2 compliant up to level 3 for securely storing keys with an elevated highest root of trust.

CipherTrust Transparent Encryption
CipherTrust Transparent Encryption delivers data at rest encryption, privileged user access controls and detailed data access audit logging. Connectors 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. The Live Data Transformation extension is available for CipherTrust Transparent Encryption, providing zero-downtime encryption and data rekeying. In addition, 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
CipherTrust Application Data Protection delivers crypto functions for 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. CipherTrust Application Data Protection accelerates development of customized data security solutions, while removing the complexity of key management from the developers' responsibility and control. In addition, it enforces strong separation of duties through key management policies that are managed only by security operations.

CipherTrust Tokenization
CipherTrust Tokenization is offered both vaulted and vaultless, and can help reduce the cost and complexity of complying with data security mandates. The vaultless offering includes policy-based dynamic data masking, whereas the vaulted offering has additional environment specific APIs. Both offerings make it easy to add tokenization to applications via RESTful APIs.

CipherTrust Database Protection
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, and IBM DB2 and Teradata databases.

CipherTrust Enterprise Key Management
CipherTrust Enterprise Key Management delivers a robust, standards-based solutions for managing encryption keys across the enterprise. It simplifies administrative challenges around encryption key management to ensure that keys are secure and always provisioned to authorized encryption services. CipherTrust Enterprise Key Management solutions support a variety of use cases including:

- **CipherTrust Cloud Key Manager** streamlines bring your own key (BYOK) management for Amazon Web Services, AWS GovCloud, Microsoft Azure, Azure Stack, Azure GovCloud, IBM Cloud, Google Cloud Platform, and Google Workspace Client-side encryption, Salesforce.com, SalesForce Sandbox and SalesForce GovCloud Plus. The solution provides comprehensive cloud key lifecycle management and automation to enhance security team efficiency and simplify cloud key management.
- **CipherTrust TDE Key Management** supports a broad range of database solutions such as Oracle, Microsoft SQL, and Microsoft Always Encrypted.
- **CipherTrust KMIP Server** centralizes management of KMIP clients, such as full disk encryption (FDE), big data, IBM DB2, tape archives, VMware vSphere and vSAN encryption, etc.

Deploy a Secure Root of Trust

Achieve compliance and scale to meet high performance use cases, by confidently securing critical environments with Thales TCT T-Series hardware security modules (HSMs)— a high-assurance, FIPS 140-2 Level 3-validated, tamper-resistant appliance. Securing the keys for data at rest and in transit, they act as trust anchors to protect the master keys that encrypt your data, digital identities, and transactions.

Thales TCT's Luna T-Series HSMs are the foundation of trust for an organization's overall ecosystem including devices, identities and transactions. 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 HSMs ensure the integrity of your cryptographic keys and functions, protecting them within a variety of form factors including a network attached appliance, an embedded PCIe card, or a portable USB appliance. Simplify integration and development with a wide variety of APIs, superior performance, and hundreds of out-of-the box technology partner applications to secure crypto key life cycles and operations.

Protect Data-in-Transit

Thales TCT offers Network Encryptors that provide network independent encryption (Layers 2, 3 and 4) for data in motion ensuring data is secure as it moves from site-to-site, or from on-premises to the cloud and back. Our network encryption solutions allow customers to better protect data, video, voice, and metadata from eavesdropping, surveillance, and overt and covert interception — all at an affordable cost and without performance compromise. Thales TCT Network Encryptors are available as both physical and virtual appliances, supporting a wide spectrum of network speeds from 10 Mbps to 100 Gbps, with platforms ranging from single to multi-port appliances.

The CN series is a hardware network appliance that delivers network layer independent (Layers 2, 3 and 4) encryption for data in motion. These hardware encryptors are certified for FIPS 140-2 Level 3 and are on the DoDIN APL.

The CV series is a hardened virtual appliance that delivers robust encryption for data-in-motion across high speed carrier WANs and SD-WAN links, using Network Function Virtualization (NFV).

Control Access to Sensitive Data and Protect User Identities

Thales TCT offers authentication solutions that address the evolution of identities. From traditional high assurance and commercial-of-the-shelf authentication solutions to first-of-a-kind hardware security module-based identity credentials, Thales TCT offers the most secure, certificate-based authentication platforms available to the U.S. Federal Government.

High Assurance Authentication

Thales TCT's high assurance authenticators bring multi-factor authentication to applications and networks where security is critical. Our certificate-based authenticators support numerous algorithms and X.509 digital certificates enabling strong two-factor authentication and proof-positive user identification in all PKI environments.

Multi-Factor Authentication

Offering the broadest range of authentication methods and form factors, Thales TCT allows customers to address numerous use cases, assurance levels, and threat vectors with unified, centrally managed policies—managed from one authentication back end delivered in the cloud or on premise.

Access Management

Thales TCT offers effective strong authentication services that enable agencies to pursue consistent authentication policies across the organization by automating and simplifying the deployment and management of a distributed estate of tokens, while securing a broad spectrum of resources, whether on-premises, cloud-based, or virtualized.

HSM-Secured Identity Credentials

Thales TCT's Luna Credential System introduces a new approach to multi-factor authentication by maintaining user 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.

Address Federal Compliance & Policy Requirements

Our industry certified solutions help address encryption and access control compliance and policy requirements such as:

- White House Cyber EO 14028
- Memo on Improving the Cybersecurity of National Security Systems
- CISA, OMB, DoD and NIST Zero Trust Initiatives
- CISA Cloud Security Technical Reference Architecture
- Dept of State- FAH: 5 FAH-8 H-354.2 Cloud Security Requirements
- DHS-CDM DEFEND
- NIST 800-53 RMF
- FISMA
- CMMC
- FedRAMP

Our products carry certifications including FIPS 140-2, Commercial Solutions for Classified program (CSfC), Committee on National Security Systems (CNSS) Memo #063-2017, and Department of Defense's Information Network Approved Product List (DoDIN APL).

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

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