Trusted Cyber Technologies

THALES
Building a future we can all trust

Data Protection Solutions for the Edge

Core-Level Security Extended to the Edge

True data protection extends to edge. Agencies need to apply the same level of security deployed in the core and the cloud to edge environments.

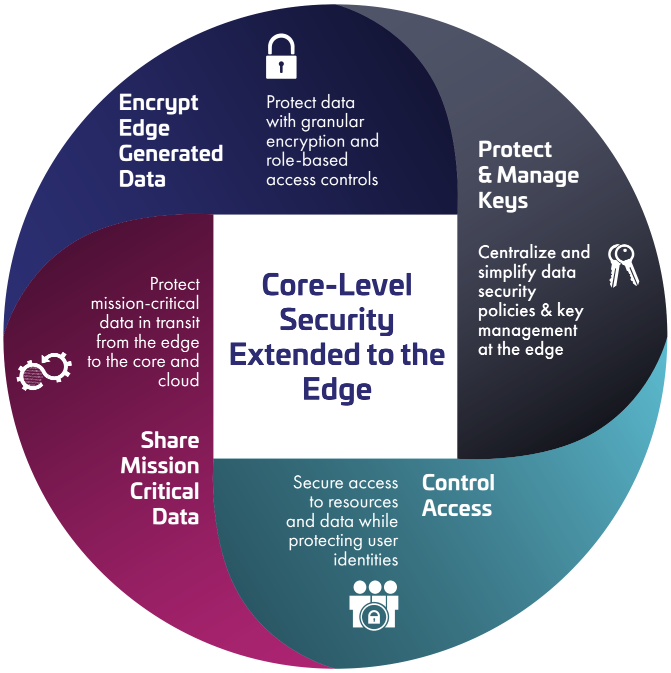
Thales Trusted Cyber Technologies (TCT), a US-based provider of cybersecurity solutions, offers unified data protection solutions that reduce the risks associated with the most critical attack vectors at the edge and solve for the government's most stringent encryption, key management, and access control requirements. Our solutions easily integrate into an existing cybersecurity infrastructure to extend your agency's data protection ecosystem to the edge. Whether integrated with a third-party product or used as standalone solution, we can tackle a wide range of mission-critical challenges. Our solutions can be cost-effectively deployed across enclave environments or scale to large number of disconnected environments.

Encrypt Edge-Generated Data

Protect data with granular encryption and role-based access controls

Thales TCT's CipherTrust Data Security Platform protects structured and unstructured data generated at the edge. CipherTrust Data Security Platform unifies data discovery, classification, data protection, and unprecedented granular access controls with centralized key management – all on a single platform.

CipherTrust Data Security Platform can be deployed at the core, the cloud, or at the edge. It simplifies data security administration with a 'single pane of glass' centralized management console that equips agencies with powerful tools to discover and classify sensitive data, combat external threats, guard against insider abuse, and establish persistent controls.



Core-Level Security Extended to the Edge

Encrypt Edge Generated Data

Protect data with granular encryption and role-based access controls

Protect & Manage Keys

Centralize and simplify data security policies & key management at the edge

Control Access

Secure access to resources and data while protecting user identities

Share Mission Critical Data

Protect mission-critical data in transit from the edge to the core and cloud

CipherTrust Transparent Encryption, offered through CipherTrust Data Security Platform, delivers data-at-rest encryption, privileged user access controls and detailed data access audit logs. Agents protect data in files, volumes, and databases on Windows, AIX, and Linux OSs across physical, virtual, and Kubernetes environments at the edge or in the cloud. CipherTrust Transparent Encryption is designed to meet data security compliance and best practice requirements with minimal disruption, effort, and cost. 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 Transparent Encryption works in conjunction with the FIPS 140 validated CipherTrust Manager, the central management point for the CipherTrust Data Security Platform, which centralizes encryption key and policy management.

Protect & Manage Keys

Centralize and simplify data security policies and key management at the edge

Thales TCT's CipherTrust k160, a compact cryptographic key management appliance, protects and manages cryptographic keys and associated policies used to encrypt the most sensitive data at rest. CipherTrust k160 provides centralized key management for a wide variety of storage partners via Key Management Interoperability Protocol (KMIP) and database partners via Transparent Database Encryption (TDE).

This cost-effective solution is ideal for small to medium sized deployments commonly found in small offices, remote sites, and tactical environments. CipherTrust k160's small form factor allows it to be easily deployed in any environment while still providing the best-in-class security features customers are accustomed to finding in the CipherTrust product family.

CipherTrust k160 includes a removable FIPS 140 validated token or a high assurance cryptographic token as its hardware root of trust. The token hardware security module (HSM) operates as a secure root of trust by encrypting all sensitive objects (e.g. keys, certificates, etc.) in CipherTrust Manager with keys that are generated by, and reside in, the token HSM. The removable token HSM provides an easy-to-use method to support common key management scenarios such as rapid key delivery disablement, key destruction, cryptographic erase, and time of use restrictions. By simply removing the detachable token you can keep mission-critical data safe, whether in the most hazardous environment or a remote branch office.

Control Access

Secure access to resources and data while protecting user identities

Thales TCT's multi-factor authentication solutions secure access to resources and data scattered across cloud, on-premises, and at the edge regardless of the end-point device being used. Thales TCT's wide range of 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 hardware tokens support physical access control to secure buildings and sites.

Allowing you to address numerous use cases, assurance levels, and threat vectors, Thales TCT authenticators are supported by authentication platforms which offer uniform, centralized policy management—delivered in the cloud or on premises. Supporting software solutions include SafeNet Trusted Access (STA) and SafeNet Authentication Service (SAS), access management and authentication services, and SafeNet Authentication Client (SAC) middleware for certificate-based authentication. Thales TCT partners with 3rd-party CMS vendors to offer the most comprehensive portfolio of identity access and authentication management solutions.

Share Mission Critical Data

Protect mission-critical data in transit from the core to the cloud to the edge.

Thales TCT network encryptors enable mission-critical information to be shared between people, organizations, locations, and communities of interest. Our FIPS 140 and DoDIN APL validated network encryption solutions provide organizations with a single platform to 'encrypt everywhere'— from network traffic between data centers, headquarters, cloud, backup and disaster recovery sites, and the edge. Ensuring maximum throughput with minimal latency, Thales TCT network encryptors allow organizations 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.

Transforming the network encryption market, Thales TCT network encryptors are the first to offer Transport Independent Mode (TIM) - network layer independent (Layer 2, Layer 3, and Layer 4) and protocol agnostic data-in-motion encryption. By supporting Layer 3, Thales TCT network encryptors offer network operators more configuration options using TCP/IP routing for securing critical data.

Thales TCT network encryptors offer flexible, vendor agnostic interoperability, meaning they're compatible with all the leading network vendors throughout your architecture. They support a wide range of security objectives and network environments, able to adapt to evolving security and network requirements. The product range supports network speeds of 10 Mbps to 100 Gbps, and platforms range from single to multi-port appliances, and are available in hardware and virtual solutions.

Supply Chain Security

Thales TCT provides US federal agencies with solutions for their cryptographic infrastructure that have a US supply chain lifecycle. Our core data protection solutions are developed, manufactured, sold, and supported in the US by Thales TCT.

We also sell and support industry-leading, third-party commercial-off-the-shelf solutions while mitigating the risk associated with procuring these solutions which are often developed outside of the US. 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 US (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.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., is a trusted, US provider of cybersecurity solutions dedicated to US 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