

Data Protection at the Edge

Extending Core-Level Security to the Environments at the Edge with Thales TCT Solutions



White Paper

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.

Core computing functionality commonly found in data centers and in the cloud is also being deployed at the edge—data protection capabilities must transition with that move.

Traditionally, data protection for civilian, intelligence, and defense agencies has been focused at the strategic, or core, level. Increasingly, it has become clear that true data protection must extend to the tactical or field-level edge. The same level of security previously reserved for strategic planning must also come into play at the edge.

Driving this push is the multi-domain transformation of federal agencies' operating environments. Take the Department of Defense for example—command posts, mobile command centers, and mobile platforms (such as vehicles, ships, and planes) are now effectively micro data centers, extending capabilities and services to the war fighter. For civilian agencies, environments at the edge such as embassies, mobile command centers, hospitals, and branch/field offices also have their own micro data centers separate from headquarters.

Many challenges often stand in the way of extending core-level security to the edge. Harsh environments; bandwidth-limited and disconnected sites; overrun or hostile scenarios; and constraints related to size, weight, and power have made it difficult to employ the appropriate levels of security while allowing the kind of quick response needed at the edge.

Edge-friendly security solutions must be able to integrate with existing cybersecurity infrastructures, either integrated with a third-party product or in a standalone application. When evaluating how to extend the data protection ecosystem to environments at the edge, a number of other considerations must also be kept in mind.



Constraints at the Edge

One of the most important aspects of providing data security at the edge is the physical environment. In a tactical scenario, the effects of dust, heat, and shock vibration exact an additional toll on computing equipment. You must consider robustness of the products you use, as well as their size, weight, and power (SWaP) requirements.

Another important concern in the physical environment is how to deal with the loss of control of the actual equipment. How do you make sure that your data is rendered useless if it falls into the wrong hands?

Military standards already provide some answers here. Many of these standards require equipment to have a small form factor and the ability to cryptographically erase information. This NIST-approved process can be used to eliminate the need to physically destroy data media following a strict sanitization process — for example overwriting drives multiple times. A cryptographic erase solution allows you to erase or destroy the keys used to encrypt data without necessarily sanitizing the storage drive itself. Under this approach, the data remains inaccessibly locked in an encrypted state, ensuring control over your data even when control over the physical equipment is lost.

In terms of the operational environment, personnel constraints introduce another difference between core and field security. In a typical data center, IT professionals and security officers are very well versed in the products with which they are working. At the edge, users may not have the same level of training. As such, products deployed to the edge need to be simple to use and configure, including support for default configurations that are secure and easy to implement.

Another key area to consider is manageability. In the core, central management systems can handle all logins, monitoring numerous pieces of equipment. This is not the case in the field, where equipment can be isolated into single units, and the environment can oscillate between connected and disconnected status back to the core. In a connected environment, where the unit is sending messages back to the central location, systems at the edge need to integrate seamlessly with the solutions running at the core. And when that connection fails or is severed, instead of sending information to a central repository, systems at the edge must be able to process and store data locally, secure it, and then (if necessary) send it back to the core once communication is reestablished.

Also under manageability, configuration and policies present their own issue sets. You need configurations that support both enterprise and local environments, and you must be able to configure units with a local interface. Then, when a given unit is plugged into a larger enterprise, or when multiple units are connected together, you need the ability to manage, configure, and set policies from the core enterprise.

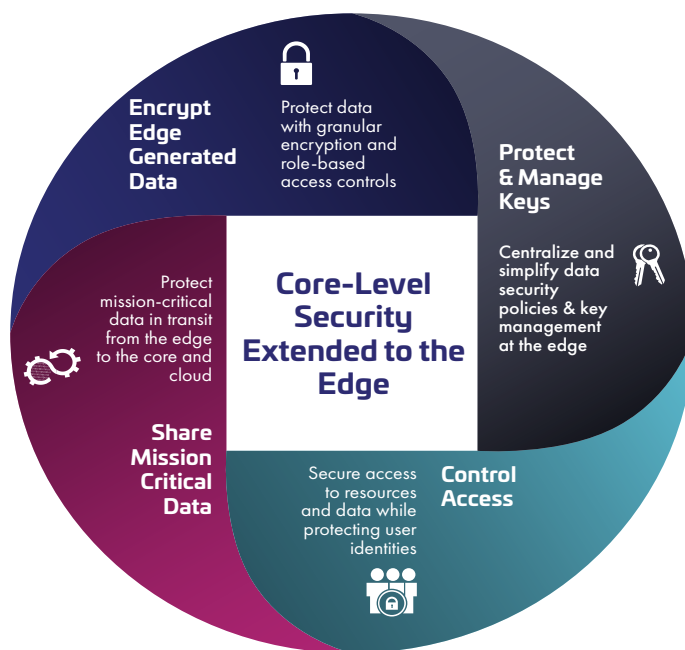
The final area is acquisition. It is important to have a strong US-based supply chain to ensure the highest levels of security. In most cases, defense organizations are constrained from purchasing security products from companies with non-US affiliations.



Core-level Security Extended to the Edge

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.

Thales TCT's approach to data protection applies the level of security deployed in the core and the cloud to edge environments. We enable agencies to:



Encrypt Edge-Generated Data

Protect data with granular encryption and role-based access controls

Sensitive data generated or stored in edge environments is continuously vulnerable to attack. Agencies need to extend core security to the edge and limit access to sensitive information to only those users, groups, and processes that require the use of the data – and no more. Agencies need to make sensitive data useless (and valueless) when not in use and allow access to the controls that make the data useful again, when it is needed by a legitimate user.

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.

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

Although data encryption at the edge is imperative, it also creates complexities for IT security teams now tasked with managing a variety of cryptographic keys. Nearly all offline data storage devices and many database management systems include the option of native encryption and onboard key management. A challenge with these islands of encryption is that keys and key management software from each provider do not usually interoperate well with one another.

The resulting silos of security create resource inefficiencies and puts the overall security posture at risk. When each system administrator separately controls encryption keys for each data repository they manage, the keys are generally stored in the same location as encrypted data. This leaves room for security compromises – the electronic equivalent of putting the house key under the doormat. Manual systems to store and transmit the encryption keys, lack of password control, and the failure to revoke keys can result in data breaches waiting to happen. And, strict adherence to compliance requirements is nearly impossible to achieve in this situation.

Centralized key management solutions enable the secure storage and backup/restore of encryption keys, define consistent access control policies, audit all key management operations, and separate encryption tasks from key management tasks.

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

Identity is the new perimeter in a perimeter-less operating environment commonly found at the edge. With apps, services, and data in the cloud and accessed through devices at the edge, everyone becomes an outsider. Establishing and enforcing a robust identity and access security policy safeguards the confidentiality, integrity, and availability of assets in the cloud, on-premises, and at the edge. At the same time, agencies can protect the privacy of their users' personal data and sustain compliance with a growing number of security and privacy regulations, laws, and jurisdictions.

New threats, risks, and vulnerabilities as well as evolving operational requirements underscore the need for a strong authentication approach based on simple service delivery, choice, and future-forward scalability.

Multi-factor authentication ensures that a user is who they claim to be. The more factors used to determine a person's identity, the greater the trust of authenticity. Because multi-factor authentication security requires multiple means of identification at login, it is widely recognized as the most secure method for authenticating access to data and applications.

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.

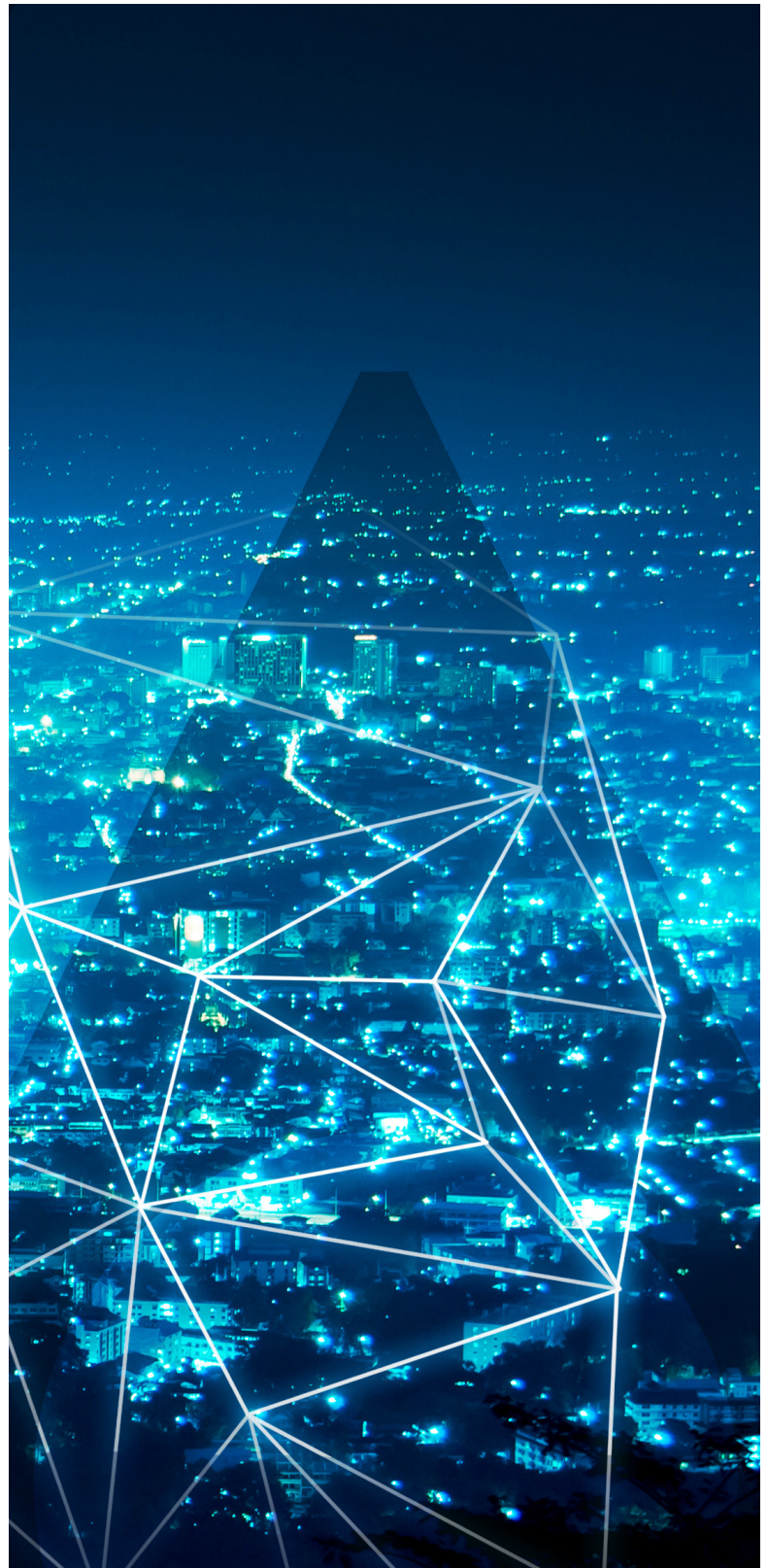
The demand for, and dependency on, high-speed wide-area networks has significantly increased over the last few years. Workloads migrating to and from the cloud, real-time global collaboration, cloud data storage, 5G and the expectation of higher bandwidth out to the edge, and the need for larger and faster aggregation points have all increased the demand on networks.

The US Federal Government's data in motion is under constant threat from bad actors—often state-sponsored—seeking to steal high-value data such as government and defense secrets through eavesdropping and data misdirection attacks. The best way to protect data in motion is to encrypt everywhere.

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.



Compliance & Policy Requirements

As environments move out to the edge, they become more susceptible to attack, making compliance with security requirements critical to minimizing vulnerability. It is important to apply the same enterprise-level security policies to the edge to ensure consistent compliance across the architecture.

Our certified data protection solutions help address encryption and access control compliance and policy requirements. Our products carry certifications including FIPS 140, 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). We address requirements including:

- White House Cyber EO 14028, National Security Memo 8
- CISA Zero Trust Maturity Model, OMB Zero Trust Strategy, DoD Zero Trust Reference Architecture, NIST Zero Trust Architecture
- DHS-CDM DEFEND
- NIST 800-53 RMF
- FISMA
- OMB Circular A-130, NIST 800-111, HIPAA

Supply Chain Security

Today's threat environment means agencies need to be completely confident in their vendors' supply chain risk management framework. From a trusted supplier perspective, you must be able to address three key questions:

- Who has had access to the development of your data security solutions?
- Do you know where your data security solutions are manufactured?
- Have the products been developed in a trusted manner?

The risk of possibly introducing malware, spyware, and backdoors from offshore cybersecurity products is not worth the small savings in cost. US-based trusted suppliers provide much needed confidence in a world where bad actors can find and exploit vulnerabilities that may be lying undetected for years, waiting for the opportunity to wreak havoc with your cybersecurity.

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

