Trusted Cyber Technologies

THALES

Thales Trusted Cyber Technologies Solutions for Continuous Diagnostics and Mitigation DEFEND

The Department of Homeland Security's (DHS) Continuous Diagnostics and Mitigation (CDM) program is designed to assess and mitigate cyber security threats across U.S. Federal civilian agencies. The program consists of four capabilities that address what is on the network, who is on the network, what is happening on the network, and how is data protected.

With phases 1 and 2 complete, civilian agencies now have identified the assets and users on their networks, attached continuous monitoring sensors to said assets, and aligned users' privileges and credentials to appropriate resources. Phase 3 built upon its predecessors and contains requirements focusing on how the network is protected. In particular, the Boundary Protection and Event Management (BOUND) tool functional area is intended to diminish inappropriate access to data, systems and networks. The requirements contain three components: BOUND-F (filtering technology), BOUND-E (encryption), and BOUND-P (physical access protection). The BOUND requirements detail the most effective methods to protect sensitive data-at-rest and in-motion via encryption and key management. Phase 3 also addresses what is happening on the network and details event management requirements, and operate, monitor and improve requirements. This includes preparedness and response to contingencies and incidents as well as the management of audit information.

Phase 4, focuses on data protection—the most critical component of an effective cyber security strategy. This phase introduces several capabilities that protect sensitive data "at rest, in use, and in transit, to ensure the confidentiality, integrity, and availability of data assets, and to ensure that sensitive information is subject to authorized access and use only".[1] It establishes protocols to identify and classify sensitive data and the location in which it resides as well as its associated data flows. Furthermore, phase 4 outlines data access controls to identify authorized users, roles, and uses.

Data Protection (DATA_PROT) requirements focus on applying protection to the data itself through encryption, access control and logging/monitoring. These encryption and key management requirements, many established under BOUND-E, include application encryption, file encryption, storage container encryption, and full disk encryption.

Thales Trusted Cyber Technologies (TCT) offers encryption and key management solutions that deliver the same level of security whether deployed in enterprise, tactical or cloud environments. Our solutions enable agencies to meet their CDM requirements while investing in a solution that provides robust security, a growing ecosystem, and the scalability needed to build a trusted framework for the future. Our solutions have a U.S. supply chain and can be deployed in any environment and easily integrate into an existing cyber security infrastructure. Thales TCT's encryption and key management solutions have received CDM Approved Product List (CDM APL) approval to address phase 3 and phase 4 requirements.

[1] https://www.gsa.gov/cdnstatic/CDM_Tech_Cap_Vol_Two_Req_Catalog_v12_2018-05-17.pdf

Why Thales TCT?

- Independent proxy company based in the U.S.
- Core customer base: U.S. Federal Government Agencies
- Maintain required Federal Government approvals and certifications to develop, support and sell products to government clients
- Provide U.S. based support for all products developed and sold through Thales TCT

Thales TCT Encryption and Key Management Solutions

Data Encryption and Key Management

Thales TCT's CipherTrust Data Security Platform offers comprehensive solutions that help government agencies address these requirements. With the CipherTrust Data Security Platform, agencies can establish strong safeguards around sensitive data and minimize critical risks associated with leaving it in an unprotected state. Thales TCT's solutions offer the controls required to ensure only authorized users can gain access to sensitive data at rest. These solutions can secure unstructured data, including documents, spreadsheets, images, web pages and more. These solutions can also secure structured data, such as fields in databases and applications that contain personally identifiable information, protected health information, mission data and other sensitive records.

With CipherTrust Data Security Platform, agencies can take a comprehensive, organization-wide approach to protecting data in support of CDM. This platform offers a number of capabilities that either comply with or exceed CDM requirements:

- **Encryption and key management.** The CipherTrust Data Security Platform offers strong, centrally managed file encryption that is transparent to processes, applications and users. The platform also delivers capabilities for efficient, centralized key management.
- **Access controls.** The CipherTrust Data Security Platform delivers advanced role-based access controls that integrate with the existing security structure for efficient deployments.
- **Multi-tenant support.** The CipherTrust Data Security Platform provides secure multi-tenancy support in the data center, cloud environments, and autonomous servers, whether they're running on Windows, Linux or UNIX. The Data Security solution enables each distinct data owner to have unique administrative functions on the centralized management appliance. This allows data that would otherwise have to be "air gapped" on separate storage devices to be cryptographically separated on shared infrastructure.
- **Privileged user controls.** With the CipherTrust Data Security Platform, security teams can establish granular controls that blind data at rest, even to individuals with privileged user account permissions, such as system administrators with root access and service account users. By leveraging these capabilities, agencies can establish strong defenses against insider threats.
- **Security intelligence.** The CipherTrust Data Security Platform delivers logs that capture attempts to access protected data, providing high-value security intelligence. These logs can be used in conjunction with a security information and event management (SIEM) solution for compliance reporting.

Network Encryption Solutions

Thales TCT's High Speed Encryption solutions provide agencies with a single platform to 'encrypt everywhere'— from network traffic between data centers and the headquarters to backup and disaster recovery sites, whether on premises or in the cloud. These solutions offer powerful safeguards for data in motion, delivering Layer 2 encryption capabilities that provide security without compromise, as well as maximum throughput and minimal latency.

Thales TCT Solutions for CDM

Requirement	Description	Thales TCT CDM APL Solution	Solution Capabilities
BOUND-E 4.1.2	Provides visibility into risks associated with the use of cryptographic mechanisms employed on an organization's network. Agencies use cryptography to protect credentials, data at rest and data in motion.	CipherTrust Data Security Platform High-Speed Encryption Appliances	The CipherTrust Data Security Platform provides protection for data-at-rest and data-in-motion. Provides data-at-rest encryption which allows access controls without changes to applications and business processes. The platform also provides a discovery process to ensure proper access is being enforced. Transparent Encryption allows data written to a protected directory to be encrypted at rest. High-Speed Encryptors provide protection for data in motion. Application Encryption and Tokenization also address security concerns around data in transit.
BOUND-E 4.1.2 Encryption as a Cryptography Technique	Encryption is a cryptographic technique used to protect against the improper disclosure of data. It ensures the confidentiality of information not be disclosed to unauthorized individuals.	CipherTrust Data Security Platform	Encryption agents run at the file system level on a server. Agents perform encryption, decryption, access control, and logging. Agents employ logic and fine-grained policies to evaluate attempts to access protected data, and then either grant or deny access. All activities are logged.

BOUND-E 4.1.2 Digital Signature Design	Digital Signature Design is used to ensure the integrity of data sent between users, to ensure the authenticity that the message is from a specific user.	CipherTrust Data Security Platform	File signing checks the authenticity and integrity of executables and applications before they are allowed to access data protected with Transparent Encryption. When file signing is initiated in the CipherTrust Manager Management Console, the Transparent Encryption Agent calculates the cryptographic signatures of the executables that are eligible to access protected data. Files are individually signed as part of a set and that set is configured in a policy that defines the processes to allow.
BOUND-E 4.1.2 Cryptographic Algorithm Element	NIST approved cryptographic algorithms for use in US Government systems are described in: • Cryptographic Algorithm Validation Program (CAVP) • NSA's Suite B cryptographic Program	CipherTrust Data Security Platform	File signing checks the authenticity and integrity of executables and applications before they are allowed to access data protected with Transparent Encryption. When file signing is initiated in the CipherTrust Manager Management Console, the Transparent Encryption Agent calculates the cryptographic signatures of the executables that are eligible to access protected data. Files are individually signed as part of a set and that set is configured in a policy that defines the processes to allow.
BOUND-E 4.1.2 Hash Element	Hash is a one-way cryptographic technique used to ensure the integrity of data, that is, to detect the alteration of the data at rest or in transit. The hash technique maps an input field of arbitrary size to a unique output field of a fixed size. The hash value of a given data can be used to determine if the original data was modified. Hash can be applied to either plain text data or cipher text data. Hash technique ensure the integrity of data at rest and in transit, and under certain designs be used to support data confidentiality (e.g., password hash).	CipherTrust Data Security Platform	Supports SHA-2 (Secure Hashing 256 bit), as well as SHA-384.
BOUND-E 4.1.2 Key Management Element	Key management is the entire process for generating, distributing using and destroying cryptographic key material. Keys are used to support the confidentiality, integrity, authenticity and secure communication between multiple users. The application of keys including digital certificates, protect against the disclosure of information, identify when data is altered and to verify the authenticity of the data source.	CipherTrust Data Security Platform	Key Management centrally manages all product keys as well as third party key material, including SSL certificates. The product leverages the CipherTrust Manager to provide an optional high availability, standards-based, FIPS 140-2 validated key management platform that can secure keys for Microsoft SQL Server TDE, Oracle TDE, and KMIP-compliant devices. The platform can manage X.509 certificates, symmetric keys, and asymmetric keys. By consolidating key management, this product fosters consistent policy implementation across multiple systems and it reduces training and maintenance costs. Key Management provides powerful and flexible administration capabilities, offering a Web interface, command-line interface, and API. The solution enables administrators to do bulk imports of digital certificates and cryptographic keys. Key Management features extensive audit capabilities that can be used to report on all activities relating to key usage, including key generation, rotation, destruction, import, expiration and export. The solution can provide alerts that help administrators stay apprised of certificate and key expiration so they can more proactively manage their environments. Key Management delivers all of the significant advantages outlined above, including high availability through system redundancy and failover.

MNGEVT 4.2	Shall have a contingency plan to restore and reconstitute full information system functionalities and the capability to apply new or additional security safeguards to prevent future compromise.	CipherTrust Data Security Platform	The CipherTrust Manager component can operate in a clustered environment in active or standby mode, and can be added to a program's COOP/DR strategy.
MNGEVT 4.2	Shall provide ongoing assessment data consolidation and assessment frequencies to deliver an effective continuous collection, analysis, and impact assessment of security policies in order to maximize automation and reduce human interaction.	CipherTrust Data Security Platform	The CipherTrust Data Security Platform processes incidents at the individual component level (host system, web GUI, CipherTrust Manager). These incidents and audit events are in an open syslog format that can be sent to an information system's monitoring/ reporting tool, including 3rd party SIEM solutions. Log file formats can be tailored to match a program's security policy for user and application behavior.
OMI 4.3	Shall collect and report information related to the implementation of methods to maintain system and information integrity and enforce system and information integrity policies.	CipherTrust Data Security Platform	Transparent Encryption provides full audit data at the CipherTrust Manager and at host agents in an open format and can integrate with a program or agency's audit reduction tool or SIEM solution.
DATA_DISCOV 5.2	DATA_DISCOV products provide consistent identification of "data assets" across the organization for processing, storing, and transmitting information at all sensitivity levels. These include: Automated Data Discovery, Data Classification, and Data Tagging	CipherTrust Data Discovery & Classification	CipherTrust Data Discovery & Classification enables scanning of systems for sensitive data. The sensitive data can be profiled based on search policies and reported on for assessment.
5.3.1 DATA_PROT _OR 1-1	Shall create and manage organizational data protection policies (e.g., cryptography, data masking/obfuscation, and access controls) using one or more PDPs.	CipherTrust Data Security Platform	The CipherTrust Data Security Platform can enforce granular access policies, enabling protection of data from misuse by privileged users and APT attacks. Granular policies can be applied by user (including administrators with root privileges), process, file type, time of day, and other parameters. Enforcement options can be used to control not only whether users can access data, but which system functions are available to a particular user. Built around a software agent that runs at the file system on a server to protect data-at-rest within structured databases or unstructured files on local or cloud-based storage. Features hardware accelerated encryption, least-privilege access controls and data access audit logging across data center, cloud and hybrid deployments. It allows controls inside of Docker and OpenShift containers, so you can ensure other containers and processes and even the host OS can't access sensitive data. Provides capabilities you need to apply encryption, access control and data access logging on a per-container basis. Live Data Transformation enables encryption and periodic key rotation of files and databases—even while in use—without disruption to users, applications and business workflows. The solution works in conjunction with FIPS 140-2 up to Level 3 validated CipherTrust Manager, which centralizes encryption key and policy management for the CipherTrust Data Security Platform.
5.3.1 DATA_PROT _OR 1-2	Shall create and manage organizational privacy protection policies that ensure privacy data is accessed, used, processed, retained, and disclosed as authorized in the cognizant Notice and applicable regulations.		
5.3.1 DATA_PROT _OR 2-1	Shall establish policies to analyze the behavior of users and endpoints related to data access and use for alignment with the data protection mechanism.		
5.3.1 DATA_PROT _OR 3-1	Shall define policies to protect data at rest using the U.S. Government approved cryptographic methods meeting BOUND-E operational and functional requirements to address one or more of the following: certificate management, application encryption, file encryption, storage container encryption, full disk encryption, or cryptographic anchoring.		

5.3.2 DATA_ PROT _FR 1-1	Shall automate the collection of audit trail information related to the creation and management of information protection policies, the execution of cryptographic methods meeting the BOUND-E operational and functional requirements for data protection, the implementation and operation of data masking/ obfuscation, and the execution of access controls enforcement of data protection policies.	CipherTrust Data Security Platform	The CipherTrust Data Security Platform produces detailed security event logs that are easy to integrate with Security Information and Event Management (SIEM) systems like Splunk, ArcSight, QRadar, and others that support syslog to produce compliance and security reports. These security logs and reports produce a non-reputable trail of permitted and denied access attempts from users and processes, providing insight into file access activities. Logging occurs at the file system level, removing the opportunity of stealthy access to sensitive data. This security information can inform of unusual or improper data access and accelerate the detection of insider and outsider threats, including the presence of APTs, and demonstrate when authorized users are performing inappropriate security-related behaviors. The CipherTrust Data Security Platform helps to provide protection across heterogeneous environments such as file systems, databases, big data implementations, VMs, cloud environments, and SAN/NAS devices. The detailed information provides in the form of RFC5424, CEF, and LEEF logs represents essential data that can be analyzed using any SIEM solution's security intelligence capabilities to identify usage patterns that may represent threats.
5.3.2 DATA_ PROT _FR 2-1	Should perform user and entity behavioral analytics that support detection of suspected compromised accounts (people or application), endpoint devices, data exfiltration, and insider access abuse (including excessive or unauthorized access to data, functions, and privilege abuse) and provide context for security investigations.		
5.3.1 DATA_PROT _FR 3-1	Shall perform cryptographic data protection, meeting BOUND-E operational and functional requirements, to reduce the risk of attacks and possible impact to data and operational processes. Cryptographic data protection may include one or more of the following: application encryption, file encryption, storage container encryption, full disk encryption, or cryptographic anchoring.	CipherTrust Data Security Platform	Transparent Encryption delivers data-at-rest encryption with centralized key management, privileged user access control and detailed data access audit logging. This protects data wherever it resides, on-premises, across multiple clouds and within big data, and container environments. The deployment is simple, scalable and fast, with agents installed at operating file-system or device layer, and encryption and decryption is transparent to all applications that run above it. Transparent Encryption is designed to meet data security compliance and best practice requirements with minimal disruption, effort, and cost. Implementation is seamless keeping both business and operational processes working without changes even during deployment and roll out. The solution works in conjunction with the FIPS 140-2 up to Level 3 validated CipherTrust Manager, which centralizes encryption key and policy management for the CipherTrust Data Security Platform.
5.3.1 DATA_PROT _FR 4-1	Shall perform data masking/obfuscation to reduce the risk of attacks and possible impact to data and operational processes. Data masking/obfuscation may include one or more of the following: substitution, shuffling, numeric variance, redaction/suppression, tokenization, format preserving encryption, or de-identification/pseudonymity.	CipherTrust Data Security Platform	Vaultless Tokenization with Dynamic Data Masking allows companies to meet PCI DSS while also making it simple to protect other sensitive data including Personally Identifiable Information (PII). And Dynamic Data Masking protects data in use while tokenization is protecting data at rest. You can efficiently address your objectives for securing and anonymizing sensitive assets—whether they reside in data center, big data, container or cloud environments. Tokenization mechanisms, methods and dynamic data masking rules are defined in a centralized, GUI. This dramatically reduces programming required for data protection. In addition, a range of format-preserving tokenization mechanisms are available to reduce requirements for changing the database schema.
5.3.1 DATA_PROT _FR 4-1	Shall implement access controls to reduce the risk of unauthorized access to sensitive (especially privacy) data through the use of one of more of the following: discretionary access control (DAC), mandatory access control (MAC), role-based access control (RBAC), attribute-based access control (ABAC),12 or adaptive access control/risk-based access control.	CipherTrust Data Security Platform	Role-based access policies control who, what, where, when and how data can be accessed. Access controls are available for system level users and groups as well as LDAP, Active Directory, Hadoop and Container users and groups. Easily implement privileged user access controls to enable administrators to work as usual, but protect against users and groups that are potential threats to data

5.3.3 DATA_ PROT Tool Functionalities	The following is a list of tool functionalities that support the Data Protection functional requirements. • Cryptographic anchoring • Discretionary access control • Mandatory access control • Role-based access control • Attribute-based access control • Application encryption • File encryption • Full disk encryption • Storage container encryption • Static data masking • Extraction-transformation-load (ETL) data masking • Dynamic data masking • Shuffling • Tokenization • Format-preserving encryption	CipherTrust Data Security Platform	The CipherTrust Data Security Platform offers capabilities for protecting and controlling access to databases, files and containers—and can secure assets residing in cloud, virtual, big data and physical environments. Capabilities include: • Transparent encryption for files, databases and containers • Application-layer encryption • Tokenization • Dynamic and static data masking • FIPS 140-2, Common Criteria certified key management • Cloud Key Management • Privileged user access control • Access audit logging • Batch data encryption and tokenization
5.5 DATA_SPIL_ FR-1-1, 1-2, 1-3, 1-4	DATA_SPIL mitigation refers to policies, processes, and procedures that an organization develops in response to an unauthorized loss of organization data.	CipherTrust Data Security Platform	Detailed data access audit logs delivered by CipherTrust Transparent Encryption are useful not only for compliance, but also for the identification of unauthorized access attempts, as well as to build baselines of authorized user access patterns. CipherTrust Security Intelligence completes the picture with pre-built integration to leading Security Information and Event Management (SIEM) systems that make this information actionable. The solution allows immediate automated escalation and response to unauthorized access attempts, and all the data need to build behavioral patterns required for identification of suspicious usage by authorized users. Leverage immediate alerts that fuel the fastest, most efficient response when issues arise. Produces an auditable trail of permitted and denied access attempts from users and processes. Uncover anomalous process and user access patterns that could point to an APT attack or malicious insider activities. Collected at the system level, CipherTrust Transparent Encryption logs report authorized and unauthorized access attempts to encrypted files and volumes-including user, time, process and more. CipherTrust Security Intelligence includes pre-built integration to leading SIEM systems that makes these logs actionable. Available dashboards immediately highlight unauthorized access attempts. Authorized user access data is available to create baselines for user's data usage, and can also be integrated with other security data such as user location and access points for pinpoint threat identification. CipherTrust Security Intelligence logs produce an auditable trail of permitted and denied access attempts from users and processes. The solution's detailed logs can be reviewed to specify when users and processes accessed data, under which policies, and if access requests were allowed or denied. In order to adhere to many compliance mandates and regulations, organizations must prove that data security is in place meets required standards. CipherTrust Security Intelligence integration to SIEM systems and pre-built dashboards can be used to easily demonstrate to an auditor that encryption, key management, and access policies are effective and appropriate. With its detailed visibility and integration capabilities, CipherTrust Security Intelligence helps streamline the effort associated with audits and ongoing compliance reporting.

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