THALES

Securely Share CUI, SBU, and Secret Data with Coalition Partners with Thales TCT Cipher Trust Data Security Platform

carahsoft

For more information, contact Carahsoft or our reseller partners:
Thales@carahsoft.com | 866-421-4683

Solution Brief

Securely Share CUI, SBU, and Secret Data with Coalition Partners with Thales TCT CipherTrust Data Security Platform

thalestct.com

THALES
Building a future we can all trust

THALES

Military operations often require unique, situational data to be shared between the U.S. and its coalition partners. Department of Defense (DoD) Zero Trust requirements dictate that data can only be shared on a need-to-know basis without blanket access for any/all coalition members. Coalition partners require the ability to limit access to sensitive information to only those users, groups, and processes that require the use of the data – and no more.

In order to protect and share data while adhering to Zero Trust requisites, coalition partners can employ a hub and spoke architecture utilizing a centralized DMZ that houses shared data. In order to ensure that mission-critical data is properly secured and shared only on a need-to-know basis, granular encryption with access controls must be deployed in the DMZ.

Data Protection through Transparent Encryption and Key Management

Thales Trusted Cyber Technologies' CipherTrust Data Security Platform (CDSP) 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 operations.

CipherTrust Transparent Encryption, a CDSP solution, 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—edge-to-cloud. Deployment is simple, scalable and fast, with agents installed at operating file system or device layer. Encryption and decryption are transparent to all applications that run above it. CipherTrust Transparent Encryption is designed to meet data security compliance and best practice requirements with minimal disruption, effort, and cost. Implementation of the encryption software is seamless, keeping operational processes working without changes even during deployment and roll out.

DoD minimally requires that all file systems, volumes, or disks be encrypted to protect data during 'powered off' scenarios. CDSP has the industry's broadest ecosystem of partners to enable central key management of those solutions. CipherTrust Transparent Encryption effectively adds a second layer of encryption that protects individual files/folders/volumes with access controls and decrypts only the requested objects at that time, for that user. This 'powered on' encryption enables granular access control to resources.

CipherTrust Manager is the common, centralized management environment for all CipherTrust Data Security Platform products. It provides policy control as well as secure management and storage of encryption keys, includes a web-based console, and enables automation through robust APIs. CipherTrust Manager is available as FIPS 140-compliant virtual and physical appliances for both enterprise and edge applications.

CipherTrust Manager can use Thales TCT's Luna T- Series HSMs as root of trust. 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. The CipherTrust Manager edge appliance uses a removable FIPS 140-certified token or high assurance token as a root of trust.

CipherTrust Manager can be configured as a multi-tenant device and can enforce strong separation of duties. Domains can be created for administrative access to CipherTrust Manager and can be assigned to individuals from each coalition partner who is responsible for their coalition's shared data. The top-level domain has the ability to control use/access from all other domains.

Each data object on the shared resource or file system will have access controls associated with it for authenticated users and is tied to their unique login account or credential such as read/write/modify/move objects, time of day, file type and other parameters.

Security Intelligence

CipherTrust Transparent Encryption and CipherTrust Manager provide extensive logging capabilities detailing successful and attempted access attempts to protected data. And, in the CipherTrust Manager management environment, agent interactions and key operations, as well as the actions of administrators at the CipherTrust Manager are also logged. Logs are designed to meet a range of needs for information from the solution.

These include:

- Audit level information required by compliance, regulatory mandates, and best practice security reports
- Immediate insight into attempted access events by users and processes that may represent threats
- Detailed historical usage data that can be used to create baselines of expected operation from access pattern recognition

These logs provide deep visibility into data access, which can be used to alert administrators to unauthorized access attempts to protected data that may represent a threat and to build typical access patterns when combined with other infrastructure and access information. These logs can be utilized by Splunk or other SEIM tools for tracking and review.

User Authentication

Users can be authenticated via trusted PKI credentials, including those from each coalition partner's PKI. Each coalition partner would therefore have their PKI trusted within the DMZ. These PKI credentials are inherently trusted and then used control access to the CipherTrust Manager, as well as the data hosting system.

Individual data objects can be tagged by their creator for access to ALL, groups, subsets of users, specific individuals. And, CipherTrust Manager uses an attribute-based access control (ABAC) model to authorize operations against protected assets.

CipherTrust Transparent Encryption Key Features

- **Transparent data protection**. Continuously enforces file-level encryption that protects against unauthorized access by users and processes and creates detailed data access audit logs of all activities without requiring changes to applications, infrastructure, systems management tasks, or business practices.
- **Seamless and easy to deploy.** CipherTrust Transparent Encryption agents are deployed on servers at the file system or volume level and support both local disks as well as cloud storage environments, such as Amazon S3 and Azure Files.
- **Define granular access controls.** Apply granular, least-privileged user access policies that protect data from external attacks and misuse by privileged users. Specific policies can be applied by users and groups from systems, LDAP/Active Directory, Hadoop and containers. Controls also include access by process, file type, time of day, and other parameters.
- **High-performance hardware accelerated encryption.** CipherTrust Transparent Encryption only employs strong, standard-based encryption protocols, such as the Advanced Encryption Standard (AES) for data encryption and Elliptic Curve Cryptography (ECC) for key exchange. Encryption overhead is minimized using the AES hardware encryption capabilities available in modern CPUs.
- **Comprehensive security intelligence.** Identify and stop threats faster with detailed data access audit logs that not only satisfy compliance requirements, but also enable data security analytics. In addition, security intelligence logs and reports streamline compliance reporting and speed up threat detection using leading security information and event management (SIEM) systems.
- **Broadest system and environment support.** The agent is available for a broad selection of Windows, Linux, and AIX platforms and can be used in physical, virtual, cloud, container, and big data environments, regardless of the underlying storage technology.

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

©2024 SafeNet Assured Technologies, LLC 78.24

THALES

Thank you for downloading this Thales TCT Whitepaper! Carahsoft is the master government aggregator and distributor for Thales TCT Cybersecurity solutions available via ITES-SW2 and other contract vehicles.

To learn how to take the next step toward acquiring [vendor]'s solutions, please check out the following resources and information:

For additional resources:
carah.io/ThalesTCTResources

For upcoming events:
carah.io/ThalesTCTEvents

For additional Thales TCT news:
carah.io/ThalesTCTNews

For additional [vertical type] solutions:
carah.io/ThalesTCTSolutions

To set up a meeting:
Thales@carahsoft.com
866-421-4683

To purchase, check out the contract vehicles available for procurement:
carah.io/ThalesTCTContracts