cpl.thalesgroup.com

THALES
Building a future we can all trust

CipherTrust Data Security Platform

Discover, Protect and Control

IT teams ask for a data-centric solution that secures data as it moves from networks to applications and the cloud. When perimeter network controls and endpoint security measures fail, data-centric solutions enable organizations to remain compliant with evolving privacy regulations and the demand to support a tremendous number of remote employees.

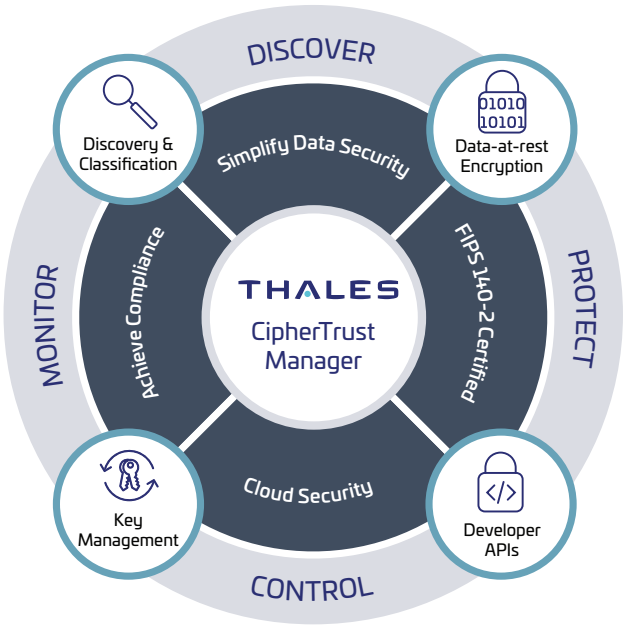
The CipherTrust Data Security Platform (CDSP) is a data-centric solution that significantly reduces risk across your business and decreases the number of resources required to maintain strong data security.

CDSP integrates centralized key management with data discovery and classification, data protection and granular access controls. By centralizing and simplifying data security, CDSP accelerates time to compliance and secures cloud migrations.

Key Features

- Centralized management console
- Monitoring and reporting
- Data discovery and classification
  - Risk analysis with data visualization
- Data discovery and classification can be combined with transparent encryption to automatically encrypt sensitive data at the file level
- Ransomware protection
  - Actively watches for malicious behavior
  - Behavior monitoring and data analytics enable:
    - Protection against zero-day attacks
    - Protection when system is disconnected from the internet
    - Protection when installed after the existence of ransomware on the endpoint
- Secrets management
  - Centralized management for all types of secrets
  - Built for ease-of-use in DevOps integrations, automations, and orchestrations
  - Manage secrets for hybrid, multi-cloud (all clouds), multi-tenants, on-prem and legacy systems and with human or machine access

- Data protection techniques
  - Transparent encryption for files, databases and big data
  - Application-layer data protection
  - Format-preserving encryption
  - Tokenization with dynamic data masking
  - Static data masking
  - Privileged user access controls
- Centralized enterprise key management
  - FIPS 140-2 compliant enterprise key management
  - Unparalleled partner ecosystem of KMIP integrations
  - Multicloud key management
  - Database encryption key management (Oracle TDE, big data, MS SQL, SQL Server Always Encrypted, etc.)



Compliance

CipherTrust Data Security Platform supports global security and privacy regulations, including:

- GDPR
- PCI DSS
- HIPAA
- SOX/GLBA
- CCPA
- FIPS 140-2
- FISMA, FedRAMP
- NIST 800-53 rev.4
- South Africa POPI Act
- ISO/IEC 27002:2013
- Japan My Number Compliance
- South Korea's PIPA
- India's Aadhaar Act
- Philippine's Data Privacy Act
- Monetary Act of Singapore
- Australia Privacy Amendment

Key Benefits

- **Simplify Data Security.** Discover, protect, and control sensitive data anywhere with next-generation unified data protection. The CipherTrust Data Security Platform (CDSP) simplifies data security administration with a centralized management console that equips organizations with powerful tools to discover and classify sensitive data, combat external threats, guard against insider abuse, and establish persistent controls, even when data is stored in the cloud or in any external provider's infrastructure for on-prem and cloud-based data. Organizations can easily uncover and close privacy gaps, detect and block ransomware, manage secrets, prioritize protection, and make informed decisions about privacy and security mandates before starting or advancing a digital transformation to fundamentally change how the organization operates and delivers value to customers.

- **Accelerate Time to Compliance.** Regulators and auditors require organizations to have control of regulated and sensitive data along with the reports to prove it. CDSP supports pervasive data security and privacy requirements such as data discovery and classification, ransomware protection, secrets management, encryption, access control, audit logs, tokenization and key management. Data security controls can be added to new deployments or in response to evolving compliance requirements. The centralized and extensible nature of the platform enables new controls to be added quickly through the addition of licenses and scripted deployment.

- **Secure Cloud Migration.** The CipherTrust Data Security Platform offers advanced encryption, centralized secrets management and centralized key management solutions that enable organizations to safely store sensitive data in the cloud. The platform offers advanced multi-cloud Bring Your Own Encryption (BYOE) solutions to avoid cloud vendor lock-in and ensure the data mobility to efficiently secure data across multiple cloud vendors with centralized cloud-agnostic encryption key management. Organizations that cannot bring their own encryption can still follow industry best practices by managing keys externally using CipherTrust Cloud Key Management (CCKM). CCKM supports Bring Your Own Key (BYOK) and Hold Your Own Key (HYOK) use-cases and streamlines Native key management across multiple cloud infrastructures and SaaS applications. CipherTrust Secrets Management powered by Akeyless Vault provides enterprise-grade secrets lifecycle management including automatic processes for creating, storing, rotating, and removing all types of secrets.

CipherTrust Data Security Platform

CDSP consists of CipherTrust Manager (CM) and a set of Connectors.

CM can be deployed on premises, in cloud or hybrid environments, or subscribed to as a service.

CipherTrust Manager

As the central management point for CDSP, CM simplifies key lifecycle management tasks for all of your encryption keys. CM manages secure key generation, backup/restore, clustering, deactivation, deletion, and access to Connectors and partner integrations that support a variety of use cases (e.g., data discovery, data-at-rest encryption, enterprise key management, and cloud key management).CM supports role-based access control to keys and

policies, robust auditing and reporting, and offers development- and management-friendly REST APIs. CM is available in both physical and virtual form factors. Hardware and virtual appliances can leverage embedded Luna Network HSMs or select cloud HSMs to enable FIPS 140-2 Level 3 highest level root of trust.

CipherTrust Data Discovery and Classification

CipherTrust Data Discovery and Classification locates regulated 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, compliance violations and prioritizing remediation. The solution provides a streamlined workflow all the way from policy configuration, discovery and classification, to risk analysis and reporting, helping to eliminate security blind spots and complexities.

CipherTrust Transparent Encryption

CipherTrust Transparent Encryption (CTE) delivers data-at-rest encryption, privileged user access controls and detailed data access audit logging. Agents 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 CTE, providing zero-downtime encryption and data rekeying. In addition, security intelligence logs and reports streamline compliance reporting and speedup threat detection using leading security information and event management (SIEM) systems.

CipherTrust Ransomware Protection

CipherTrust Transparent Encryption Ransomware Protection (CTE- RWP) monitors behaviors, watching for suspicious activities and blocks processes when ransomware indicators are detected. Using behavior monitoring and data analytics rather than malware signature databases, CTE-RWP protects systems from zero-day attacks even when disconnected from a network. Exceptionally easy to deploy and manage.

CipherTrust Secrets Management powered by Akeyless Vault

CipherTrust Secrets Management (CSM) is a state-of-the-art, enterprise-grade secrets management solution powered by the Akeyless Vault Platform. CSM protects and automates access to secrets across DevOps tools and cloud workloads including credentials, certificates, API keys and tokens. DevSecOps can quickly and easily integrate secrets management into multi-cloud applications to secure and speed-up continuous integration and continuous delivery processes. Exceptionally easy to deploy and manage.

CipherTrust Intelligent Protection

CipherTrust Intelligent Protection enables organizations to rapidly discover and classify data based on sensitivity, vulnerability, and risk profiles and pro-actively protect at-risk data using encryption and access controls. It integrates CipherTrust Data Discovery and Classification with CipherTrust Transparent Encryption to improve operational efficiencies, accelerate time to compliance, and pro-actively close security gaps.

CipherTrust Application Data Protection

CipherTrust Application Data Protection (CADP) delivers crypto functions such as 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 so that developers can move quickly to secure data processed in their applications. CADP accelerates development of customized data security solutions, while removing the complexity of key management from developer responsibility and control. In addition, CADP 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 such as PCI-DSS. Tokenization replaces sensitive data with a representative token, so that the sensitive data is kept separate and secure from the database and unauthorized users and systems. The vaultless offering includes policy-based dynamic data masking. Both offerings make it easy to add tokenization to applications.

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, IBM DB2 and Teradata databases.

CipherTrust Key Management

CipherTrust Key Management delivers a robust, standards-based solution 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 Key Management solutions support a variety of use cases including:

- **CipherTrust Cloud Key Management (CCKM)** streamlines "Bring Your Own Key" (BYOK), "Hold Your Own Key" (HYOK) and Native key management for Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure[1], Oracle Cloud Infrastructure (OCI)[1], Salesforce and SAP[1]. CCKM increases efficiency by reducing the operational burden – even when all of the cloud keys are Native keys. Giving customers lifecycle control, centralized management within and among clouds, and visibility of cloud encryption keys, reduces key management complexity and operational costs.
- **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.

1 Check with us for dates for HYOK support for this cloud.