Data Sheet

CipherTrust Data Security Platform

Thales offers a unified approach to data security

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

CipherTrust Data Security Platform

You can discover, protect and control your organization's sensitive data to avoid the security breaches that are happening with alarming regularity. The CipherTrust Data Security Platform from Thales enables you to protect your data and meet the data protection compliance mandates that are becoming more stringent. To stay a step ahead of dynamic cybersecurity threats, your organization needs to extend data protection across more environments, systems, applications, processes and users with a data-centric solution. A data-centric solution secures data as it moves from networks to applications and the cloud, and decreases the number of resources required to maintain strong data security.

The CipherTrust Data Security Platform (CDSP) significantly reduces risk across your business. CDSP integrates centralized key management with data discovery, classification, data protection and granular access controls. CDSP decreases resources required for data security operations and compliance controls by simplifying data security, accelerating time to compliance, and securing cloud migration.

The CDSP platform offers capabilities for discovering, protecting and controlling access to databases and files—and can secure assets residing in cloud, virtual, and physical environments. This scalable, efficient data security platform enables you to address your urgent requirements and prepares your organization to respond nimbly when the next security challenge or compliance requirement arises.

Capabilities

- 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
  - Multi-cloud key management
  - Transparent Data Encryption (TDE) key management

Environments

- Clouds: Amazon Web Services, Google Cloud Platform, IBM Cloud, Microsoft Azure, Oracle Cloud Infrastructure, Salesforce, SAP, and more
- Supported OSs: Linux, Windows and Unix
- Big Data: Hadoop, SAP HANA
- Database: IBM DB2, Microsoft SQL Server, MongoDB, MySQL, Oracle, Sybase, Teradata and others
- Any storage environment

Platform advantages

- Discover, protect and control your organization's sensitive data anywhere with next-generation unified data protection
- Consistent security and compliance across physical, virtual, and cloud environments
- Identify and secure data across structured, unstructured and big data platforms
- Reduce time-to-value. Rapidly enable platform capabilities as needed
- Hardware Security Modules as the secure root of trust for the platform include FIPS 140-2 Level 3 certification

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 for on-prem and cloud-based data. Organizations can easily uncover and close privacy gaps, 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, 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 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 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 across multiple cloud infrastructures and SaaS applications. CCKM provides a single pane of glass view for each of the public clouds, showing all regions in a single pane of glass and removing the need for SMEs to become experts in every cloud system.With the CipherTrust Data Security Platform, the strongest safeguards protect an enterprise's sensitive data and applications in the cloud, helping the organization meet compliance requirements and gain greater control over their data, wherever it is created, used or stored.

Featured products:

CipherTrust Manager (CM) is the central management point for the CDSP platform, providing data access and key policy management. CM is available in both physical and virtual form factors that are up to FIPS 140-2 Level 3 compliant.

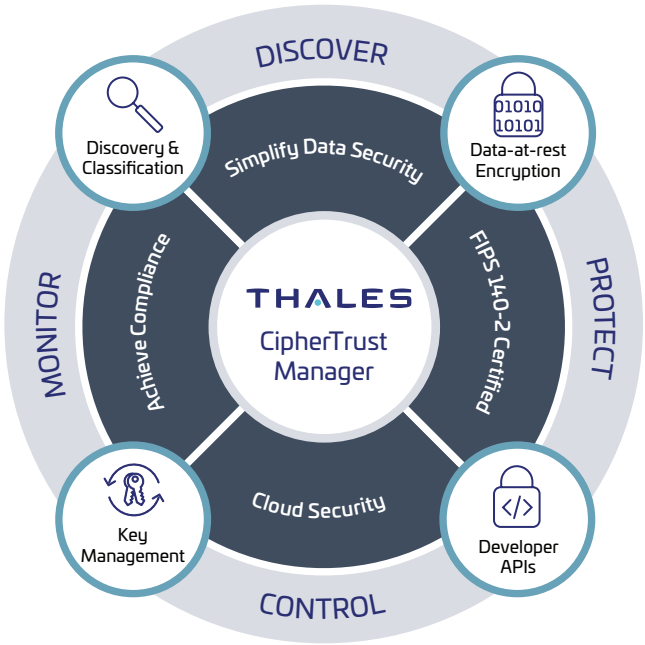
Data Discovery and Classification (DDC) enables organizations to discover and classify sensitive data from a single pane of glass. Organizations can understand risks, uncover gaps, and make better decisions about both third-party data sharing and cloud migration.

CipherTrust Enterprise Key Management manages encryption keys for many sources and environments across the enterprise, simplifying encryption key management across storage, databases and clouds. The CipherTrust KMIP Server operates on CipherTrust Manager to centralize key management for many KMIP clients and partner-verified solutions. CipherTrust Application Key Management (CAKM) is available for Oracle TDE and Microsoft SQL Server EKM. CipherTrust Cloud Key Management (CCKM) streamlines Native key management, Bring Your Own Key" (BYOK) and "Hold Your Own Key" (HYOK) for Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure[1], Oracle Cloud Infrastructure (OCI)[1], Salesforce and SAP[1].

Data-at-Rest Encryption protects data without requiring any changes to business or data management processes. CipherTrust Transparent Encryption (CTE) encrypts data across environments and platforms (on-premises, cloud, database and big data platforms) with comprehensive data access controls that can stop even the most damaging attacks. CTE provides a single pane of glass view and consistent configuration across guardpoints. Extensions such as Live Data Transformation enable zero-downtime data encryption and key rotation.

The CipherTrust Data Security Platform offers a range of products with developer-friendly application programming interfaces for Key Management, Encryption and Tokenization. CipherTrust Application Data Protection provides server- or RESTful API-based key management and encryption services. CipherTrust Tokenization solutions include both Vaultless Tokenization with Dynamic Data Masking and Vaulted Tokenization based on use-case requirements.

CipherTrust Database Protection (CDP) solutions provide database column-level encryption without the need for software engineering assistance. CDP solutions deliver the highest level of separation of duties for access to sensitive data.



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

CipherTrust Manager

Overview

At the center of the CipherTrust Data Security Platform (CDSP) is CipherTrust Manager. CipherTrust Manager (CM) centralizes keys, management and policies for all of the CDSP Connectors:

- Data Discovery and Classification
- Enterprise Key Management
- Cloud Key Management
- Transparent Encryption
- Live Data Transformation
- Application Data Protection
- Database Protection.

Built on an extensible microservices architecture, CM enables organizations to efficiently address privacy and data protection regulatory mandates and adapt readily as encryption and IT requirements evolve.

CM simplifies key lifecycle management including key generation, backup and restore, deactivation and deletion. Core features of CM: role-based access to keys and policies, multi-tenancy support, robust auditing and reporting of both key usage and operational changes.

CM is available in both virtual and physical appliance form factors to address varying deployment use cases from public and private clouds to on-prem secure deployment with physical security controls. 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.

Active/Active clustering for the highest availability can be configured with a mix of hardware and virtual appliances. Active/Active clustering provides customers with high-assurance deployments ensuring 24x7 uptime to support key management and data encryption requirements.

Key benefits

- Centralized key management allows consolidation of on-prem and cloud encryption keys across multiple applications, data stores, and appliances
- Provides the foundation for the Ciphertrust Data Security Platform, enabling customers to reduce business risk with data discovery, classification and protection of sensitive data
- Simplifies management with a self-service licensing portal and visibility into licenses available and in use
- Cloud-friendly deployment options with support for Alibaba Cloud, AWS, Azure, Google Cloud, OpenStack, Oracle Cloud, VMware and more
- Superior key control and generation via Hardware Security Module (HSM) integrations
- Extensible microservices architecture enabling maintenance and upgrades without downtime
- Unparalleled partner ecosystem of integrations with leading enterprise storage, server, database, application and cloud vendors

Key features

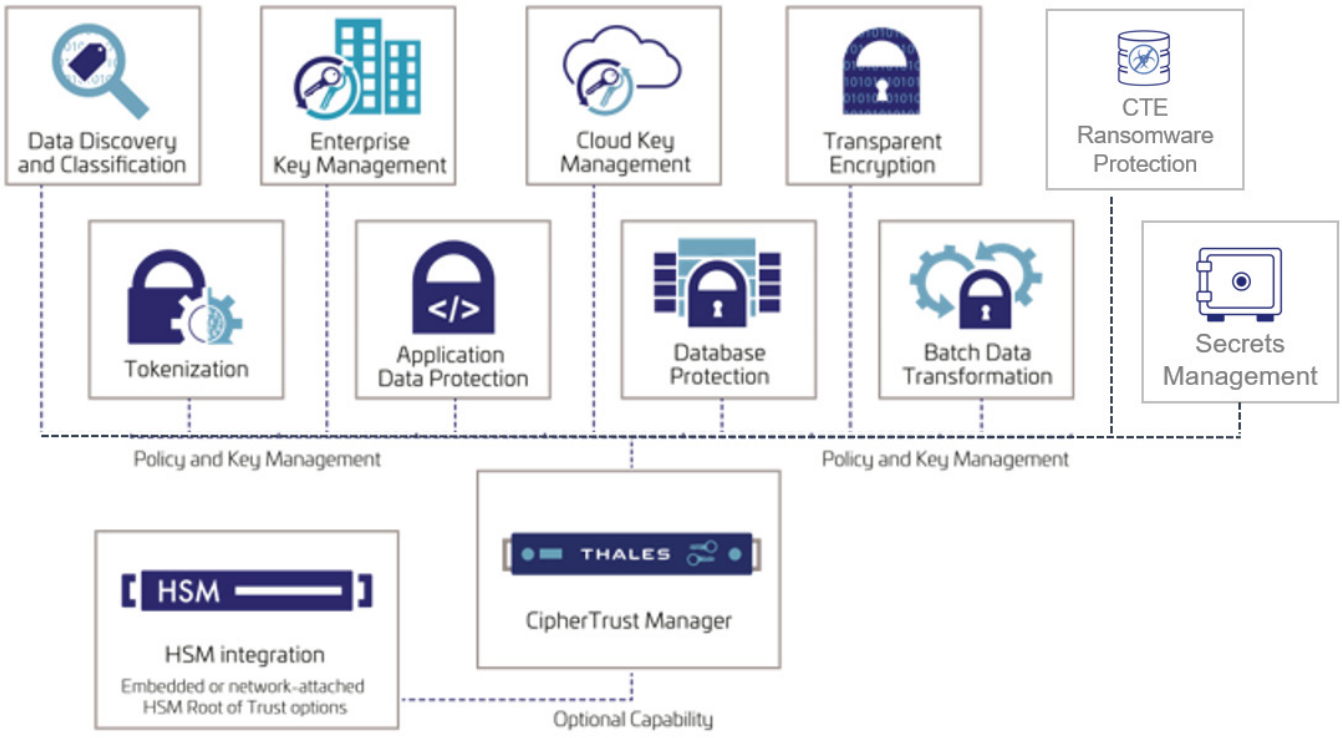
- Full Key Lifecycle Management, including secure key generation, rotation, deactivation, deletion, and backup/restore
- Centralized administration, unifying key management operations with role-based access control and full audit log review
- Self-service licensing, streamlining Connector license provisioning and ongoing management
- Secrets management, providing the ability to create and manage secret and opaque objects for use on the platform
- Multi-tenancy provides capabilities required to create multiple domains with separation of duties to support large enterprise environments
- REST APIs to automate repetitive management and encryption tasks
- Flexible HA clustering and intelligent key sharing, offering clustering physical and/or virtual appliances
- Robust auditing and reporting, including tracking key state changes, administrator access, and policy changes in multiple log formats (RFC-5424, CEF, LEEF) for easy

THALES

Unified management and administration across the hybrid enterprise

CipherTrust Manager minimizes total cost of ownership by providing central management of heterogeneous encryption keys, including keys generated for CipherTrust Data Security Platform products, Microsoft SQL TDE, Oracle TDE and KMIP-compliant encryption products. CipherTrust Manager features an intuitive web-based console and APIs for managing encryption keys, policies, and auditing across an enterprise.

For CipherTrust Manager Features, Appliance Specifications, Safety Certifications and Emissions Certifications, please refer to the CipherTrust Manager Product Brief.



CipherTrust Transparent Encryption - Ransomware Protection

CipherTrust Transparent Encryption - Ransomware Protection (CTE-RWP) provides active behavior monitoring and data analytics to protect sensitive data from ransomware attacks. CTE-RWP watches files hosting business-critical data, looking for abnormal I/O activity on a per process basis. It allows administrators to alert or block suspicious activity before ransomware can control your endpoints/servers.

Transparent Data Protection

CTE-RWP continuously enforces ransomware protection enabled per disk volume with minimal configuration and no modification to any applications on the endpoint/server. It continuously monitors abnormal file activity caused by ransomware-infected processes, and alerts/blocks when abnormal file activity is detected.

Easy to Deploy

CTE-RWP enables administrators to configure ransomware protection without setting up CTE restrictive access control and encryption policies on a per file/folder basis.

Robust Ransomware Detection

CTE-RWP uses process-based machine learning models to dynamically detect suspicious file I/O activity. It identifies and alerts or blocks ransomware on endpoints/servers. A trusted list for permitted processes can be set up to avoid unwanted monitoring or blocking.

Managed in CipherTrust Manager

CTE-RWP can be licensed separately or in conjunction with CTE. When CTE-RWP is combined with a CTE license, administrators can additionally apply fine-grained access control and encryption.

Key benefits

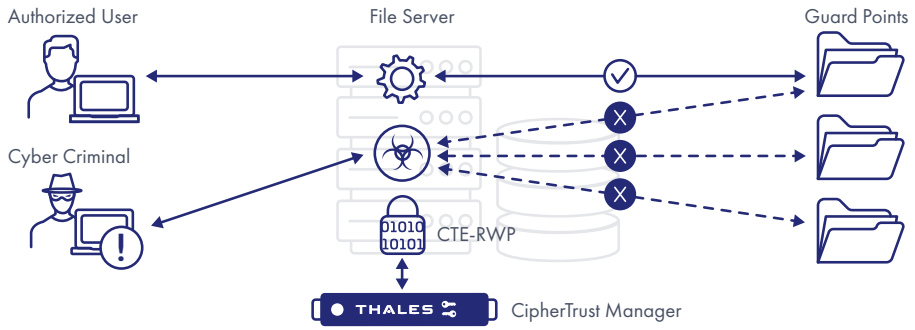
- Able to detect zero-day attacks (unknown malware)
- Detects ransomware activity – even if installed after the existence of ransomware on the endpoint
- Continuously enforces ransomware protection per disk volume regardless if the system is connected to the internet or not
- Easy-to-deploy protection with minimal configuration, no modification to applications on the endpoint and no setup of access controls or encryption policies

Key features

- Monitors abnormal I/O activity caused by ransomware-infected processes and alerts/blocks the malicious activity when detected
- No depencencies on malware signature databases
- Enabled per disk volume; monitors both local and cloud (SMB/CIFS shares) volumes
- A trusted list for permitted processes can be set up to avoid unwanted monitoring or blocking

Technical specifications

- Requires CipherTrust Manager v2.12 and CipherTrust Transparent Encryption v7.4.0 and subsequent versions
- Windows platform (Linux on roadmap)
- IP addresses, routing configurations, and DNS addresses must allow connectivity to CipherTrust Manager
- Communication between CipherTrust Manager and the CTE Agent defaults to port 443



CipherTrust Transparent Encryption - Ransomware Protection (CTE-RWP)

(Applicable when licensed with or without CTE)

CipherTrust Secrets Manager

CipherTrust Secrets Management (CSM) powered by Akeyless Vault is a state-of-the-art enterprise-grade secrets management solution which protects and automates access to secrets including credentials, certificates, API keys, and tokens across DevOps tools and cloud workloads.

Centralized Secrets Management

Manage static and dynamic secrets, specify rotation schedules, manage API keys, SSH keys, and other credentials to eliminate risk of secrets sprawl.

Easy to Deploy

CipherTrust Secrets Management (CSM) is easily accessible from the CipherTrust Manager dashboard. The total cost of ownership is low because CSM can be configured within minutes without special training so setup happens sooner and faster, and is easy to maintain.

Seamless Integrations

Built with DevOps in mind, CSM easily integrates with third party applications such as GitHub, Kubernetes, Open Shift and other applications popular within the DevOps community.

Scalability for hybrid and multi-cloud

Moving to the cloud is often a protracted transition, resulting in hybrid environments, with some resources on premises, and others distributed across multiple public and private clouds. CSM works in hybrid, multi-cloud (all clouds), multi-tenant, on-prem and legacy systems and with human or machine access.

Key benefits

- Centralized management for all types of secrets
- Easy-to-use, automated functionality for DevSecOps
- Decreased time to compliance with automation, orchestration and audit logs
- Low total cost of ownership (TCO) – SaaS application with no hidden costs for infrastructure, time, resources or support
- Log reporting and analytics for auditing and compliance

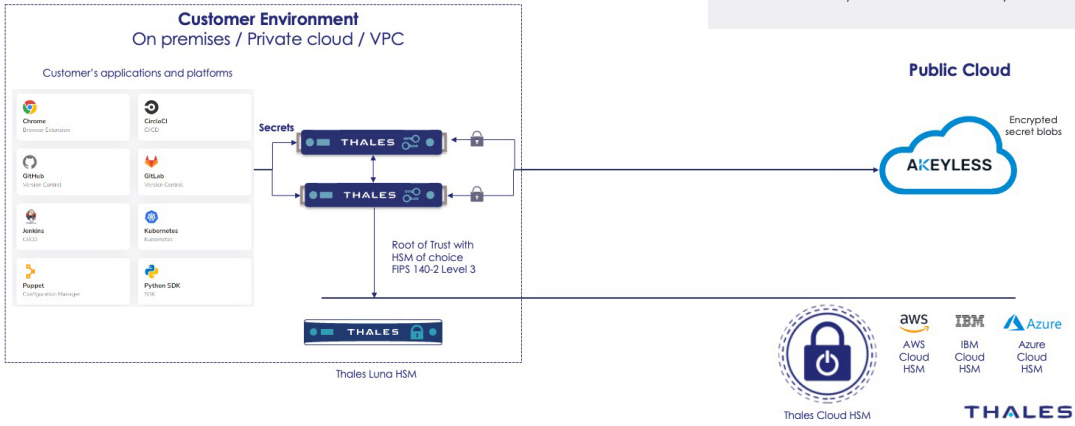
Key features

- Manages all types of secrets
- Automated processes for creating, storing, sharing, rotating and removing secrets
- Dynamic, just-in-time secret generation and management
- Access secrets management through CipherTrust Manager – the unified console to access multiple tools in the data security platform to discover, protect and control your data.
- FIPS 140-2 Level 3 Root of Trust with HSMs

Technical specifications

- SaaS secrets vault platform with gateway to CipherTrust Manager
- Supports encryption keys, static secrets, rotated secrets, dynamic secrets, SSH cert issuers, PKI cert issuers and certificates
- CipherTrust Manager's encrypted customer fragment (an AES256 key) of every secret is protected by the same root of trust key hierarchy protecting all keys originating from CipherTrust Manager. This is in addition to the benefits of Akeyless' Distributed Fragments Cryptography™ (DFC) technology
- Interfaces include: Gateway configuration manager, gateway console, REST APIs (v1 & v2), CLI
- Integration categories include: Browser Extensions, CI/CD, Code Management, Configuration Management, Identity Providers, Infra Automation, Kubernetes, Notification apps and SDKs

CipherTrust Secrets Management Deployment



CipherTrust Data Discovery and Classification

Data Discovery and Classification (DDC) 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, prioritizing remediation, and securing your cloud transformation.

Data Discovery and Classification provides a streamlined workflow from policy configuration, discovery and classification, to risk analysis and reporting, helping to eliminate security blind spots and complexities.

Enterprise-wide data privacy

CipherTrust DDC delivers an enterprise-wide data privacy solution that is simple to deploy and scale. It provides ready-to-use templates and a streamlined workflow to help you quickly discover your regulated data across traditional and modern repositories.

Single pane of glass for clear visibility

DDC provides a clear understanding of sensitive data, usage, and risks of exposure, from a single pane of glass. A centralized console with visualized data and aggregated reports enables informed decisions about data sharing, digital transformation, and prioritizing remediation.

Quick start with flexibility

Data Discovery and Classification provides a comprehensive set of built-in classification templates for commonly requested data privacy and security regulations, such as GDPR and CCPA, while easily handling custom policies based on specific patterns, algorithms and more.

Demonstrate compliance

CipherTrust Data Discovery and Classification provides detailed reports that can demonstrate compliance with various regulations and laws. Efficient scans build a strong foundation for overall data privacy and security to auditors.

Flexible deployment options

DDC is available in both agent-based and agentless deployment modes. The choice enables security and IT teams to select deployment modes for optimal results and efficient cost of ownership.

Key benefits

- Reduce complexity and risk with streamlined workflows unique to your organization
- Privacy officers can rapidly uncover privacy gaps, prioritize remediation, and proactively respond to regulatory and business challenges from a single pane of glass
- Build a strong foundation for overall data privacy and security through effective scans that help discover both structured and unstructured data across a diverse set of data stores
- Ensure secure third-party data sharing by scanning for sensitive data and removing it, as needed, in advance

Data Discovery and Classification Technical specifications

- Data Stores
- Local storage and local memory on the host
- Network storage
  - Windows Share (CIS/SMB)
  - Unix File System (NFS)
- Databases
  - IBM DB2
  - Oracle
  - SQL
- Big Data
  - Hadoop Clusters

Type of files supported

- Databases: Access, DBase, SQLite, MSSQL MDF & LDF
- Images: BMP, FAX, GIF, JPG, PDF (embedded), PNG, TIF
- Compressed: bzip2, Gzip (all types), TAR, Zip (all types)
- Microsoft Backup Archive: Microsoft Binary/BKF
- Microsoft Office: v5, 6, 95, 97, 2000, XP, 2003 onwards
- Open Source: Star Office/Open Office
- Open Standards: PDF, HTML, CSV, TXT

Type of data identified

- Health (Australian Medicare Card, European EHIC, US Health Insurance Claim number, etc.)
- Financial (American Express, Diners Club, Mastercard, VISA card numbers, bank account number, etc.)
- Personal (name, last name, address, DOB, email, etc.)
- National ID (social security number, Spanish DNI, etc.)
- Custom information types

Pre-built templates

The solution includes a wide range of ready-to-use templates that can help you meet common regulatory and business policy needs:

- CCPA
- GDPR
- HIPAA
- PCI DSS
- PII
- PHI

Minimum RAM required

- 16GB

Minimum Network Connection

- 1GB

CipherTrust Enterprise Key Management

CipherTrust key management products centralize key management for CipherTrust Connectors, 3rd party devices, databases, cloud services and applications. With CipherTrust's centralized key management, organizations increase their control of encryption keys and data security, connecting with applications through standard interfaces.

Enterprise key management solutions

CipherTrust Enterprise Key Management solutions support a variety of applications, including:

Key Management Interoperability Protocol (KMIP)

KMIP is an industry-standard protocol for encryption key exchange between clients (appliances and applications) and a server (key store). Standardization facilitates external key management for storage solutions including SAN and NAS storage arrays, self-encrypting drives and hyper-converged infrastructure solutions. KMIP simplifies the requirement of separating keys from the data being encrypted, enabling keys to be managed with a common set of policies. CipherTrust Manager operates in the KMIP Server role for a broad range of third-party applications and devices operating in the KMIP client role.

Database Management

CipherTrust Application Key Management (CAKM) for databases can provide high security while providing enhanced IT efficiency. CAKM is installed in the database to request keys from CipherTrust Manager and serve them to Oracle TDE or Microsoft SQL Server EKM interfaces.

Key Management for Proprietary Applications

For the most convenient integrations with applications that perform encryption and require centralized key management, CipherTrust Manager offers developer-friendly API's that can be leveraged in a wide range of application environments. For the most performance-sensitive applications, CipherTrust Application Data Protection offers application-layer libraries implementing Java, C, C++, .NET and .NET Core with key management "providers" for Microsoft Crypto API (CAPI), Crypto Next-Generation (CNG) and Crypto Services Provider (CSP) plus PKCS#11.

Key Management Technical specifications

Administration

- Secure-web, CLI, API
- Command line scripts

Key Formats for Search, Alerts, and Reports

- Symmetric encryption key algorithms: AES, ARIA
- Asymmetric key algorithms
  - RSA
  - Elliptic Curve: brainpool, prime, secp

Third-Party Encryption

- Microsoft SQL Server EKM, Microsoft SQL Always Encrypted, Oracle TDE

API Support

- PKCS#11
- Microsoft Crypto API (CAPI), Cryptographic Service Provider (CSP), Cryptographic Next Generation Provider (CNG), Java Cryptographic Extension (JCE), Microsoft Extensible Key Management (EKM)
- KMIP

Key Availability and Redundancy

- Secure replication of keys across multiple appliances with automated backups

Verified KMIP Integrations

HCI

- Cloudian HyperStore, VMware vSAN/VMCrypt, Nutanix, Dell EMC ECS, NetApp Cloud ONTAP, Hedvig Distributed Storage Platform, Dell EMC PowerOne, Dell EMC PowerFlex

Backup

- Commvault Data Protection Advanced

Mainframe

- Syncsort Assure Encryption for IBM i-Series

Storage

- DellEMC Data Domain, DellEMC PowerEdge, NetApp FAS, HPE Proliant/StoreEasy (iLO)*, HPE 3PAR, HPE Primera, IBM DS8000 Series

Flash Storage

- Dell EMC PowerMax, IBM , Dell EMC PowerStore

Tape Libraries

- HPE StoreEver, Quantum Scalar series

Database/Big Data

- MongoDB, IBM DB2, Oracle MySQL

*integrated via NAE-XML API

CipherTrust Cloud Key Management

CipherTrust Cloud Key Management (CCKM) reduces key management complexity and operational costs by giving customers lifecycle control, centralized management and visibility of cloud encryption keys.

Customer key control

Industry best practices as defined by the Cloud Security Alliance (CSA) require that keys be stored and managed outside of the cloud service provider and the associated encryption operations[1]. Cloud Service Providers (CSPs) can comply with best practices by offering Bring Your Own Key (BYOK) or Hold Your Own Key (HYOK) services to enable customer control of the keys used to encrypt their data. Customer control of the keys allows for the separation, creation, ownership and control, including revocation, of encryption keys or tenant secrets used to create the keys.

Key benefits

- Gain higher efficiency with centralized key management across hybrid, single-and multi-cloud environments, including key discovery, management of Cloud Native keys and automated key rotation
- Amplify the benefits of Cloud Native keys by using a robust multi-cloud platform with outstanding UI
- Leverage the value of "Bring Your Own Key" and "Hold Your Own Key" services with full lifecycle cloud encryption key lifecycle management
- Comply with the most stringent data protection mandates with secure key origination

Enhanced IT efficiency

Capabilities supporting IT efficiency include

- Centralized access to each cloud provider from a single browser window
- Management of Cloud Native keys
- Automated synchronization ensuring that cloud console operations are centrally visible
- Automated key rotation with support for expiring keys which can save thousands of hours per year

Encryption key security

Customer key control requires secure key generation and storage.

CCKM leverages the security of CipherTrust Manager, Luna Network HSM, or the Vormetric Data Security Manager (DSM) to create keys with up to FIPS 140-2 Level 3 security.

Compliance tools you need

Key activity logs and prepackaged reports enable fast compliance reporting. Logs may be directed to multiple syslog servers or SIEM systems.

1 See CSA CCM EKM-04

Single Pane of Glass

Access to each cloud provider from a single console, across multiple accounts, regions, subscriptions and projects makes it easier for organizations to understand how their workloads across different clouds are protected. We continually increase key visibility to make it easier for administrators to manage and control access to the keys in minutes instead of days, and stop threats faster.

Supported clouds and key management ownership models:

Amazon Web Services (AWS) KMS	Native	BYOK	
AWS CloudHSM	Native		
AWS XKS			HYOK
AWS China	Native	BYOK	
AWS GovCloud	Native	BYOK	HYOK
Google Cloud Platform CMEK	Native	BYOK	
Google Cloud Platform EKM			HYOK
Google Cloud Platform EKM UDE			HYOK-CC*
Google Workspace CSE			HYOK
Microsoft Azure Cloud	Native	BYOK	
Microsoft Azure China	Native	BYOK	
Microsoft Azure GovCloud	Native	BYOK	
Microsoft Azure Managed HSMs	Native	BYOK	
Microsoft Office 365		BYOK	
Oracle Cloud Infrastructure	Native	BYOK	HYOK
Salesforce.com	Native	BYOK	HYOK **
Salesforce Sandbox	Native	BYOK	HYOK **
SAP Data Custodian	Native	BYOK	

Flexible Deployment Options

Deployment environments include: public cloud, private cloud, hybrid cloud, physical appliances and an as-a cloud-based subscription service.

* HYOK-CC is HYOK for Confidential Computing
** Cache-only Key Service

CipherTrust Transparent Encryption

CipherTrust Transparent Encryption (CTE) delivers data-at-rest encryption with centralized key management, granular access controls and data access logging that helps organizations meet compliance reporting and best practice requirements for protecting data.

The solution's transparent approach protects structured databases and unstructured files, across multiple cloud environments, and within big data implementations. Implementation is seamless – keeping both business and operational processes unchanged.

Meet compliance requirements

Encryption, access controls and data access logging are basic requirements or recommended best practices for almost all compliance and data privacy standards and mandates, including PCI DSS, HIPAA/Hitech, GDPR and many others. CipherTrust Transparent Encryption delivers the required controls.

Scalable encryption

CipherTrust Transparent Encryption runs at the file system or volume level on a server, and is available for Microsoft Windows Server, many variants of Linux, and IBM AIX operating systems. It can be used in physical, virtual, cloud, and big data environments – regardless of the underlying storage technology. Administrators perform all policy and key administration through CipherTrust Manager.

Server-based encryption eliminates bottlenecks with both performance and scalability further enhanced by leveraging cryptographic acceleration built into CPUs, such as Intel AES-NI and IBM POWER.

Granular access controls

Granular, least-privileged access policies protect data from external attacks and privileged user misuse. Policies can be applied by users and groups from systems, LDAP/Active Directory, and Hadoop. Controls include process, file type and other parameters.

Access policies can be defined to create a permitted list of "trusted" applications to prevent any untrusted binaries (e.g., ransomware) from accessing data stores protected by CipherTrust Transparent Encryption and to prevent privileged users from accessing user data in files and databases. These access policies can block any rogue binaries from encrypting files/databases, even if the intruder has execute permissions for that binary and read/write permission to the target file that contains business critical data.

Non-intrusive, transparent deployment

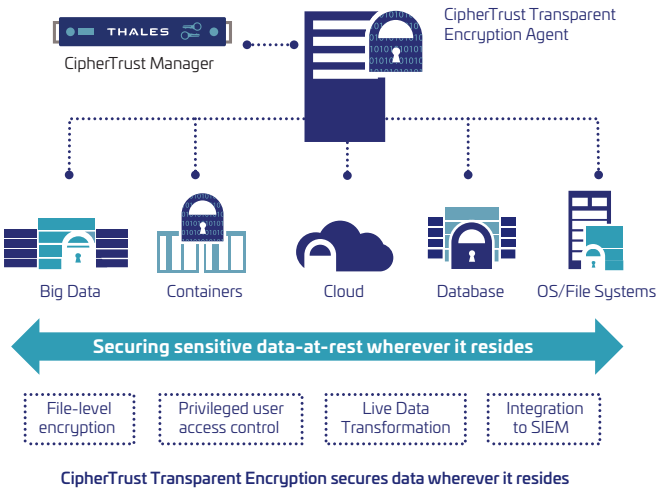
The solution requires no changes to applications, workflows, business or operational procedures.

Key benefits

- Meet compliance and best practice requirements for encryption and access control that scales
- Easy to deploy: no application customization required
- Establish strong safeguards against abuse by privileged insiders and malware using stolen credentials

Key features

- Broadest platform support in industry: Windows, Linux and AIX operating systems
- High performance encryption: Uses hardware encryption capabilities built into host CPUs - Intel, AMD AES-NI and IBM POWER AES encryption
- Logs permitted, denied and restricted access attempts from users, applications and processes
- Role-based access policies control who, what, and how data can be accessed
- Enable privileged users to perform work without access to clear-text data



CipherTrust Transparent Encryption secures data wherever it resides

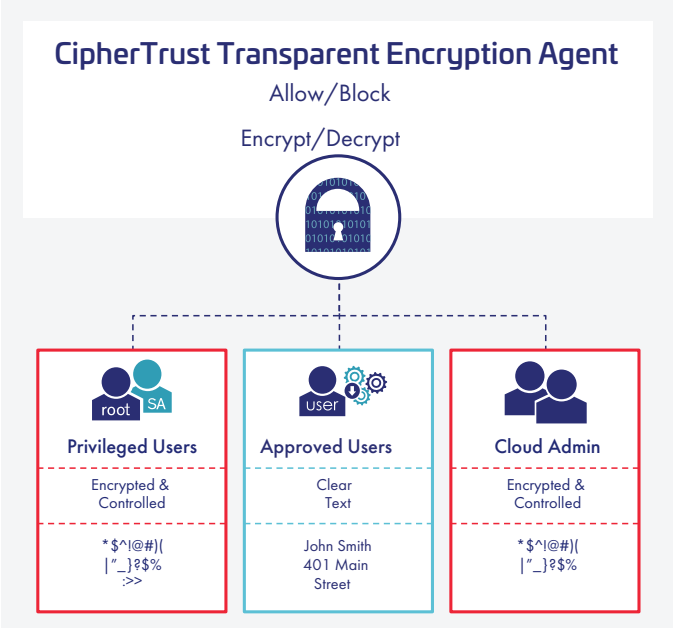
Protect data on-premises or in-cloud

Cloud data security might seem easy at first. Turning on the equivalent of full-disk encryption for a public cloud provider is simple. But it's a multi-cloud world. Managing data security across multiple public clouds and different cloud storage options quickly gets complex. CipherTrust Transparent Encryption enables you to secure your cloud data with controls and keys centralized and common across multiple infrastructure as a service (IaaS) clouds – handling more threats than cloud-native can address.

CipherTrust Transparent Encryption protects nearly any storage mapped to IaaS environment operating systems. And with advanced data protection for Amazon S3, organizations can apply transparent encryption and access controls to sensitive data in S3 buckets. The solution encrypts unstructured files, semi-structured data, or structured databases before they are written to Amazon S3 buckets. The solution works in conjunction with the FIPS 140-2 up to Level 3 compliant CipherTrust Manager, assuring strong separation of key and policy management from the data. Once an S3 bucket is guarded with CTE, any file deposited in it is automatically encrypted, and the data inside is rendered useless in the event of unauthorized access. With CipherTrust Transparent Encryption's support for Amazon S3, organizations can ensure that volumes of data stored in the cloud are safe and comply with the strictest security regulations while helping to close the cloud industry's most common security gaps.

Security Intelligence

CipherTrust Transparent Encryption in concert with CipherTrust Manager provides insight into file access activities. Data access logging includes detail on both authorized data access and unauthorized access attempts wherever CTE is operating. Information provided also includes actions of security administrators – another item required for compliance audit purposes.



CipherTrust Transparent Encryption Technical specifications

Encryption Algorithms and Capabilities

- AES

Extension Licenses

- Live Data Transformation

Platform Support

- Microsoft: Windows Server 2022, 2019 and 2016
- Linux: Amazon Linux, Red Hat Enterprise Linux (RHEL), SuSE Linux Enterprise Server, Ubuntu
- UNIX: IBM AIX

Database Support

- IBM DB2, Microsoft SQL Server, Microsoft Exchange
- Data Availability Group (DAG), MySQL, NoSQL, Oracle, SAP, Sybase, Teradata and others

Application Support

- Transparent to all applications, including SAP, SharePoint, custom applications and more

Big Data Support

- Hadoop: Cloudera, IBM
- NoSQL: Couchbase, DataStax, MongoDB
- SAP HANA

Encryption Hardware Acceleration

- AMD and Intel AES-NI
- IBM POWER9 cryptographic coprocessor

Agent Certification

- FIPS 140-2 Level 1

Cloud Support

- AWS: EBS, EFS, S3, S3I, S3 Glacier
- AZURE: Disk Storage, Azure Files
- GCP: Persistent Disk, Local SSD, Filestore

Security Intelligence logs are forwarded to SIEM systems via SYSLOG or CEF among other protocols to speed up threat detection.

Data sets can also be used to create access pattern baselines which can then be used to rapidly identify threats represented by behavior deviating from baseline.

CipherTrust Transparent Encryption Extensions and Additions

CipherTrust Live Data Transformation

Data-at-rest encryption deployment and management can present challenges during initial encryption or when rekeying data that has already been encrypted, requiring either planned downtime or data cloning and synchronization. Live Data Transformation for CipherTrust Transparent Encryption (CTE LDT) enables encryption and rekeying with unprecedented uptime and administrative efficiency.

Zero-downtime encryption and key rotation

Administrators can encrypt data without downtime or disruption to users, applications or workflows. While encryption is underway, users and processes continue to interact with databases or file systems as usual.

Security best practices and regulatory mandates require periodic key rotation. Live Data Transformation addresses these requirements with speed and efficiency through online key rotation and data rekeying.

CTE LDT provides resource management capabilities to balance between encryption and business demands. An administrator can define a rule specifying that, during business hours, encryption can only consume 10% of system CPU, while on nights and weekends, encryption can consume 70% of CPU. Similar controls are available for I/O operations.

CTE LDT offers faster backup and archive recovery. In a data recovery operation, archived encryption keys recovered from CipherTrust Manager are automatically applied to an older data set. Restored data is encrypted with the current cryptographic keys.

CipherTrust Transparent Encryption for SAP HANA

CTE safeguards SAP HANA data enabling enterprises to meet rigorous security, data governance, and compliance requirements. The solution enforces strong data encryption on all SAP HANA data and log partitions and protects and controls access to the SAP HANA Persistence layer. The solution can be quickly deployed and requires no changes to SAP HANA or the underlying database or hardware infrastructure. Further, SAP has reviewed and qualified CipherTrust Transparent Encryption as a suitable solution for SAP HANA 2.0 environments.

Key benefits

- Zero-downtime encryption and key rotation
- Efficient online key rotation and data rekeying
- Resource management to balance between encryption and business demands
- Faster backup and archive recovery
- Centrally managed
- Enforces policies/compliance
- Secures data at rest

CipherTrust Transparent Encryption for Teradata

CipherTrust Transparent Encryption for Teradata (CTE for Teradata) is a high performance encryption solution for Teradata databases. A CTE agent on the host allows root users to do their job, without abusing data by applying block-level encryption, access control and data audit logging. CipherTrust Manager manages CTE for Teradata and prevents unwanted processes from accessing the Teradata database(s). CipherTrust Manager centralizes encryption key and data access policy management.

CipherTrust Transparent Encryption for UserSpace

CTE UserSpace provides a robust and scalable file system level encryption and access control solution for the variety of flavors of Linux servers in the distributed enterprise without changes to infrastructure or applications. Once CTE UserSpace is deployed, files containing sensitive data are rendered useless in the event of a breach, misuse or hijacking of privileged accounts, physical theft of servers, and other potential threats.

CipherTrust Transparent Encryption for Kubernetes

CTE for Kubernetes (CTE K8s) can apply data protection (including encryption, user and process-based access controls, and data access logging) on a per-container basis, both to data inside of containers and to external persistent volume storage accessible from containers.

CipherTrust Tokenization

Tokenization reduces the cost and effort required to comply with security policies and regulatory mandates such as the European Union's Global Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI-DSS). CipherTrust Tokenization offers application-level tokenization services in two convenient solutions that deliver complete customer flexibility: Vaultless Tokenization with Dynamic Data Masking and Vaulted Tokenization. Both solutions secure and anonymize sensitive assets—whether they reside in the data center, big data environments or the cloud.

Vaultless Tokenization

CipherTrust Vaultless Tokenization protects data at rest while its policy-based Dynamic Data Masking capability protects data in use. A RESTful API in combination with centralized management and services enables tokenization implementation with a single line of code per field. Vaultless Tokenization is provided by dedicated, distributed-cluster-capable Tokenization Servers, offering full separation of duties. Tokenization management and configuration including an operational dashboard with convenient tokenization configuration workflows occurs in a graphical user interface.

Dynamic Data Masking. Policies define whether a tokenized field is returned fully-or partially-masked based on user identification controlled by an AD or LDAP server. For example, the policies could enable customer service representatives to see only the last four digits of credit card numbers, while account receivables staff could access the full credit card number.

Non-disruptive. Format preserving tokenization protects sensitive data without changing the database schema.

Vaultless Tokenization Technical specifications

Tokenization capabilities:

- Format-preserving tokens with irreversible option
- Random tokens data length up to 128K
- Date tokenization
- Unicode UTF-8 character set support enable data tokenization in almost any language
- Luhn checking option for FPE and random tokens

Dynamic data masking capabilities:

- Policy based, number of left and/or right characters exposed, with customizable mask character
- Authentication with Lightweight Directory Access Protocol
- (LDAP) or Active Directory (AD)

Deployment Form Factors and Options:

- Open Virtualization Format (.OVA) and International
- Organization for Standardization (.iso)
- Microsoft Hyper-V VHD
- Amazon Machine Image (.ami)
- Microsoft Azure Marketplace
- Google Cloud Platform

System requirements:

- Minimum hardware: 4 CPU cores, 16–32 GB RAM
- Minimum disk: 80GB

Application integration:

- RESTful APIs

Performance:

- More than 1 million credit card size tokenization transactions per second, per token server (using multiple threads and batch (or vector) mode) on a 32-core server (dual-socket Xeon E5-2630v3) with 16 GB RAM

Vaulted Tokenization

CipherTrust Vaulted Tokenization also offers non-disruptive format preserving tokenization with a wide range of existing formats and the ability to define custom tokenization formats. Vaulted Tokenization provides a high level of security for highly sensitive data, and instances of it may be installed on a per-server basis or installed as a web service supporting multiple clients.

Fast integration

CipherTrust Tokenization solutions are rapidly integrated with minimal software engineering, leveraging standard protocols and environment bindings.

Vaulted Tokenization Technical specifications

Tokenization capabilities:

- Format-preserving tokens
- Random or Sequential token generation
- Purge specific tokens on demand, equivalent to purging original data
- Masked: Last four, First six, First two, etc.
- Fixed length and width masking
- Customer defined custom formats
- Regular expressions (Java style)

Supported Token Vault Databases

- Microsoft SQL Server
- MySQL
- Oracle
- Cassandra

Application integration

- RESTful APIs
- .NET
- Java

CipherTrust Application Data Protection

Overview

CipherTrust Application Data Protection (CADP) offers DevSecOps-friendly software tools for key management operations, as well as application-level encryption of sensitive data. The solution is flexible enough to encrypt nearly any type of data passing through an application. Protecting data at the application layer can provide the highest level of security, as it can take place immediately upon data creation or first processing, and can remain encrypted regardless of its data lifecycle state – during transfer, use, backup or copy. CADP can be deployed in physical, private or public cloud infrastructure to secure data even when it is migrating from one environment to another, without any modifications to existing encryption or data processing policies.

CADP is deployed with CipherTrust Manager, an architecture that centralizes key and policy management across multiple applications, environments, or sites. The combined solution provides granular access controls that separate administrative duties from data and encryption key access. For example, a policy can be applied to ensure that no single administrator can make a critical configuration change without additional approval.

CADP features built-in, automated key rotation, and offers a wide range of cryptographic operations including encryption, decryption, digital signing and verification, secure hash algorithms (SHA), and hash-based message authentication code (HMAC).

CipherTrust Application Data Protection is rich in function and provides both development and, and operational flexibility:

Functional richness is delivered in the form of built-in server health checking and failover coupled with multi-tiered load balancing and built-in key rotation.

Development flexibility is delivered with REST, C/C++, .NET Core, Net and Java cryptographic libraries to enable creation of crypto applications for the widest range of programming skills.

Operational flexibility is twofold:

First, a broad range of cryptographic providers are available including native C through Crypto API (CAPI), PKCS#11, the Cryptographic Service Provider (CSP) and Crypto Next Generation (CNG) Providers for Windows and the Java Crypto Engine (JCE).

Second, **encryption operational flexibility** is delivered by the choice to encrypt locally or on CipherTrust Manager, for the library or Web Service edition of the product, without changing any code.

The choice is implemented with a simple configuration change.

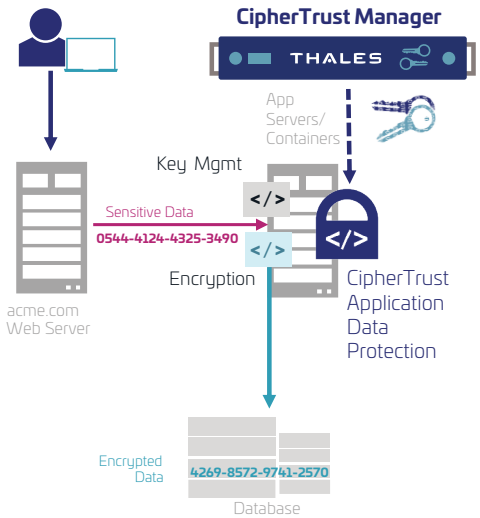
Where to encrypt involves choices and potential benefits:

- Encryption on CipherTrust Manager offers security, performance, and scalability benefits, and for the highest level of security, ensures that keys never leave the trusted CipherTrust Manager. Offloading encryption from application servers can enable them to perform better. Embedded in CADP libraries are load-balancing mechanisms that enable an encryption load to be spread across a cluster of CipherTrust Managers.
- Encryption on the application server can provide potentially higher performance for certain types of encryption workloads. In contrast to open-source solutions, keys are encrypted in memory when not in use, and scattered in memory when in use. Both mechanisms secure crucial encryption keys from abuse.

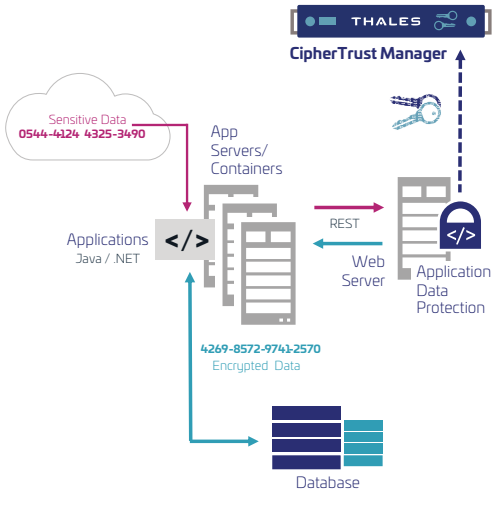
CADP in concert with CipherTrust Manager provides a single interface for logging, auditing, and reporting access to protected data and encryption keys.

Rich Encryption Ecosystem

In addition to the key management integrations discussed above, CipherTrust Application Data Protection has integrations for Microsoft Crypto Next Generation (CNG), Microsoft Crypto Service Provider (CSP), Microsoft Online Certificate Status Protocol (OCSP), Hashi Vault, HortonWorks, Apache HTTP and NGINX Servers, Lieberman ERPM, and many others.



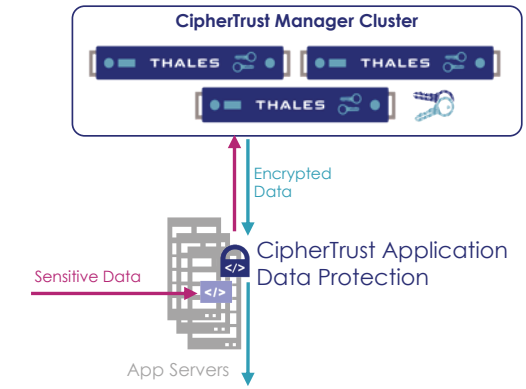
CipherTrust Application Data Protection with Installable Libraries

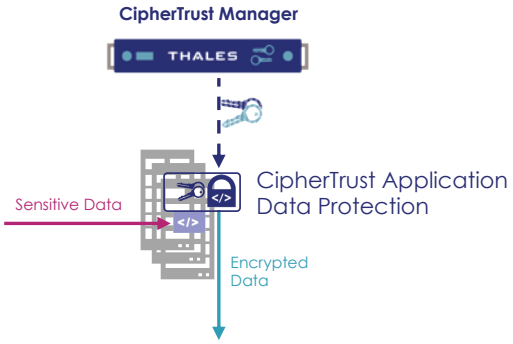


CipherTrust Application Data Protection installed as a Web Service

Key benefits

- Centralized key management, freeing developers from complex and risky key management stores
- Strengthen security and ensure compliance
- Leverage the cloud with utmost security
- Accelerate security application development
- Optimize application server performance
- Unparalleled partner ecosystem of integrations with leading enterprise storage, server, database, application and cloud vendors
- Key management for a broad range of native encryption solutions





Application Data Protection Technical specifications

Development Libraries and APIs

- Java, C, and C# for .NET Core and .NET
- KMIP standard
- XML open interface W
- Web services: REST

Crypto Service Providers and Supported OS's C provider

- Windows
- AIX
- Linux
- MacOS

KMIP Server/Provider

- On CipherTrust Manager

PKCS#11 provider

- Windows Server
- AIX
- Linux
- Solaris

Java Crypto Extension Provider

- Windows Server
- HP-UX
- Linux
- AIX
- Solaris

CSP and CNG Providers

- Windows Server 2008 and up

Encryption Algorithms

- 3DES, AES 256 (CBC and XTS), SHA 256, SHA 384, SHA 512, RSA 1024, RSA 2048, RSA 3072, RSA 4096,

ECC

- Format-preserving: FF1/FF3, Tokenization

Web Application Servers

- Apache Tomcat, IBM WebSphere, JBoss, Microsoft IIS, Oracle WebLogic, SAP NetWeaver, Sun ONE, and more

Cloud and Virtual Infrastructures

- Works with all major cloud platforms, including AWS, Azure, IBM Cloud, Google and VMware

CipherTrust Database Protection

Overview

CipherTrust Database Protection (CDP) products provide transparent column-level encryption of structured, sensitive data in databases (e.g., credit card, social security numbers, national ID numbers, passwords, email addresses). CipherTrust Database Protection offers convenient choices in database protection and leverages CipherTrust Manager for centralized key management. CDP is configured centrally on the CipherTrust Manager console.

The CDP solution enables you to efficiently protect and secure sensitive data fields in databases. CDP solutions are transparent and cloud-friendly, requiring no changes to applications or business processes. For efficiency, CDP offers a simple configuration change to choose between encrypting locally, for performance, or remotely in CipherTrust Manager, to ensure that encryption keys never leave the secure enclave.

CipherTrust Database Protection

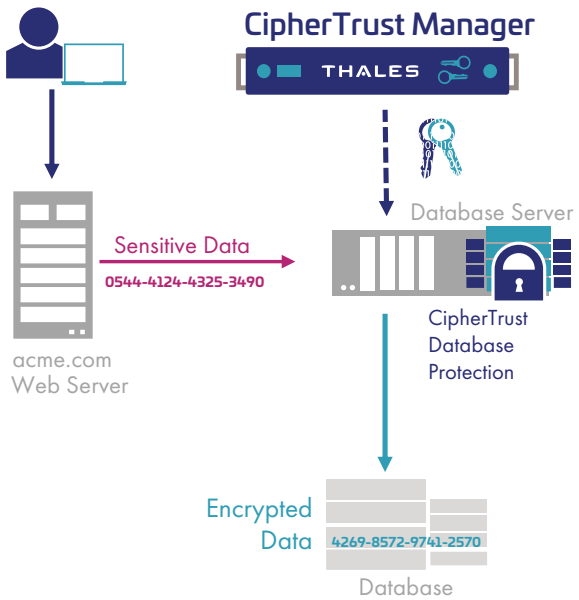
CipherTrust Database Protection encrypts data, leveraging database views and triggers to ensure that access to nonencrypted and encrypted fields remains transparent to applications. Key granularity is on a per-field basis.

Deployment and initial use

CipherTrust Database Protection is installed on each database server. It can be installed manually or through a silent installer.

Once installed, CDP is securely linked to CipherTrust Manager for access to keys, configurations and remote encryption and decryption services.

Installation is usually followed by a data migration process involving selection of data, defining database schema, view and trigger design, and finally bulk data encryption.



Database Protection Technical specifications

Supported Databases

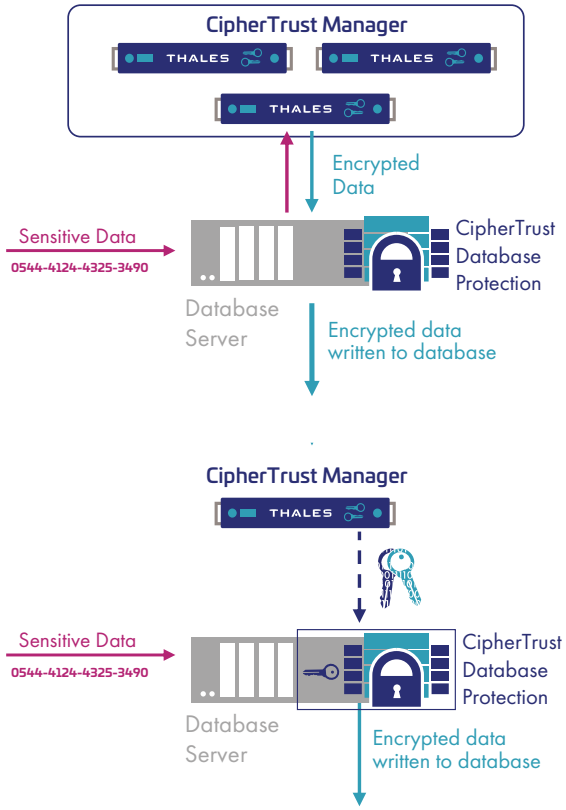
- Oracle
- Microsoft SQL Server
- IBM DB2

Supported Platforms

- Microsoft Windows
- Linux
- Solaris
- AIX

Encryption Algorithms

- FPE (FF1, FF3), AES, 3DES, RSA, ECC



Once installed, CDP triggers and views enable

- new data to be encrypted
- database reads to be decrypted for permitted users
- database updates to be encrypted with full transparency to users and workflows

Where to encrypt when using CipherTrust Database Protection involves choices and potential benefits:

- For the highest level of security, encryption on CipherTrust Manager offers security, performance, and scalability benefits, and ensures that keys never leave the trusted CM. Offloading encryption from database servers can enable them to perform better. And, embedded in CipherTrust Database Protection are load-balancing mechanisms that enable an encryption load to be spread across a cluster of CipherTrust Managers.
- For potentially higher performance for certain fields of database encryption, you can encrypt on the database server. In contrast to open-source solutions, keys are encrypted in memory when not in use, and scattered in memory when in use. Both mechanisms protect crucial encryption keys from abuse.

CipherTrust Teradata Protection

CipherTrust Teradata Protection (CTP) simplifies the process of securing sensitive columns in the Teradata Vantage SQL Database. To minimize the potential impact of data protection on associated applications and workflows, and avoid the increased storage requirements of conventional encryption approaches, CTP offers both traditional encryption and NIST-approved format-preserving encryption (FPE) capabilities, enabling protection of fields without altering their format. Dynamic data masking enables different levels of decryption and presentation of data to specific users.

Streamline encryption deployment and usage

The CTP solution reduces potential complexity arising from data protection for Teradata Vantage SQL as user-defined function (UDF) in the database engine, enabling data access to be controlled separately by database users and administrators.

Security administrators specify data access profiles defining encryption methods and user-specific alllow- and deny-lists. The solution also enables the use of different encryption keys per database column, and then binds unique keys to one or more Teradata Vantage Database users. Specific deny behaviors are also available on a per-user basis. Once data is encrypted, the data remains protected even if UDFs are disabled administratively.

Technical specifications

Supported Databases

- Teradata Database, minimum version 16.2

Supported Platforms

- SUSE Linux Enterprise Server (SLES) minimum version 11 SP3

Encryption Algorithms

- AES, FPE (FF1, FF3)

Maximum Column Widths

- ASCII—16KB, Unicode—8KB

Encryption Controls

- Identity-based access per column
- Dynamic masking based on identity

Allow/Deny access controls Encryption Key Sources

- CipherTrust Manager

Key benefits

- Boost security without compromising the value of big data analytics
- Establish protections against cyber attacks and abuse by privileged users
- Fast, convenient deployment and configuration

CipherTrust Batch Data Transformation

Static Data Masking

To use data sets while preventing misuse of sensitive data, Static Data Masking transforms selected data into unreadable forms.

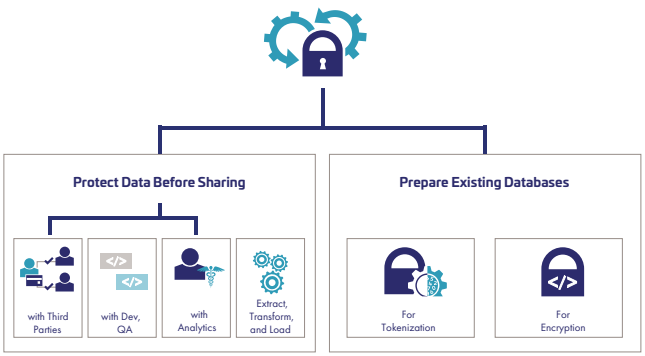
CipherTrust Batch Data Transformation (BDT) offers high-performance data masking with centralized encryption key management, leveraging CipherTrust Application Data Protection (CADP) and CipherTrust Vaultless Tokenization (CT-VL) to protect vast quantities of data quickly.

Static Data Masking has many use cases, such as:

1. Prior to sharing data with third parties.
2. In databases shared with development, QA, R&D or analytics.
3. Before adding a data set to a big data environment.
4. In advance of extract, transform and load (ETL) operations.

Other use cases include

- Preparing a database for a tokenization or encryption deployment
- Rekeying an encrypted column of data after key rotation



CipherTrust Batch Data Transformation for High-Volume Flexible Data Masking, Tokenization and Encryption

Key benefits

- Secure, cost-effective static data masking with centralized data encryption keys from sources hardened up to FIPS 140-2 Level 3
- Enable database sharing with reduced risk
- Accelerates protection of existing data following deployment of CipherTrust Data Discovery and Classification
- Static data masking where you need it. Deploy on premises, in the cloud, or as a hybrid deployment.

Technical specifications

Data Transformation Options:

- Tokenization, Data Encryption
- Formatting, preserving alpha/numeric

Policy File Options:

- Specific action for each individual column transformation –Encrypt, decrypt, tokenize, de-tokenize and re-key
- Easy to apply encryption without the need for application changes
- Flexible key management options – keys in CipherTrust Manager or server, multiple key support

Data Security Platform Requirements

- Key sources: CipherTrust Manager, Vormetric Data Security Manager, KeySecure Classic
- Pre-requisite components: Tokenization requires CipherTrust Tokenization Server deployment and license; Encryption requires either CipherTrust Application Data Protection or Vormetric Application Encryption and license

Hardware and Operating System Requirements:

- Processor with 4 cores, 16GB RAM (minimum)
- Java Runtime Environment (JRE)
- Windows Server 2012 minimum
- Linux – RedHat, CentOS, Ubuntu and SUSE

CipherTrust Intelligent Protection

CipherTrust Intelligent Protection

CipherTrust Intelligent Protection (CIP) is an all-in-one solution designed to simplify and strengthen your organization's data security. CIP discovers and classifies data based on sensitivity, vulnerability, and other risk profiles and proactively protects at-risk data using encryption and access controls. CIP is a solution configuration within the Thales CipherTrust Data Security Platform that leverages CipherTrust Manager, CipherTrust Data Discovery and Classification, and CipherTrust Transparent Encryption.

Accelerate time to compliance

Secure your organization's sensitive data and comply with ubiquitous data security and privacy requirements under GDPR, CCPA, PCI-DSS, HIPAA, and other evolving regulatory and industry mandates.

Build operational efficiency with integrated workflows

Simplify data security operations and strengthen data protection with automated compliance workflows that enable you to discover, classify and encrypt in a single step when new sensitive data is found.

Uncover and close security gaps

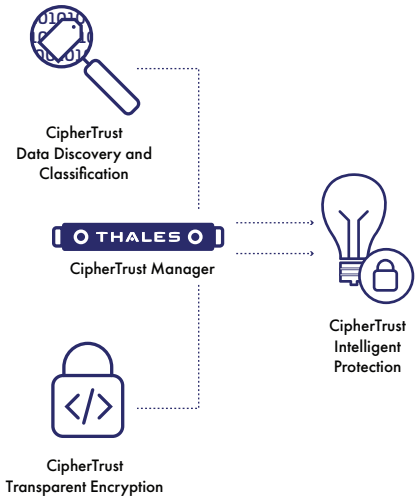
Uncover security gaps and apply the most appropriate data protection techniques to proactively protect data based on vulnerability and risk profiles.

Key benefits

- Locate both structured and unstructured sensitive data across the entire enterprise in multi-cloud, big data, relational databases, or file storage systems
- Classify sensitive data—such as national IDs, financial data, and personal data—based on built-in templates or market-proven classification techniques
- Leverage rich visualizations and risk scores to help you decide what additional protection is needed for data identified and classified as being at risk
- Proactively remediate risk using automated workflows and data protection techniques, such as encryption and access controls

Key features

- Rapid discovery and classification of both structured and unstructured sensitive data across the entire enterprise in multi-cloud, big data, relational databases, or file storage systems
- Built-in classification profile templates and infotypes are constantly kept up to date to reflect the latest mandates
- Configurable policies protect at-risk data using encryption and granular access controls
- Detailed charts and reports provide risk analysis, status, and alerts throughout the data lifecycle
- Highly scalable solution designed to keep pace with data growth



cpl.thalesgroup.com

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us