Braxton-Grant TECHNOLOGIES

THALES

CipherTrust Data Security Platform

Discover, protect and control sensitive data anywhere with next-generation unified data protection

Discover Protect Control

Data Sheet

CipherTrust Data Security Platform

As security breaches continue to happen with alarming regularity and data protection compliance mandates get more stringent, your organization needs to extend data protection across more environments, systems, applications, processes and users. With the CipherTrust Data Security Platform from Thales, you can effectively discover, protect and control your organization's sensitive data anywhere with next-generation unified data protection. CipherTrust Data Security Platform is available for sale exclusively through Thales Trusted Cyber Technologies (TCT)

The CipherTrust Data Security Platform integrates data discovery, classification, data protection and granular access controls, all with centralized key management. This solution removes data security complexity, accelerates time to compliance, and secures cloud migration, which results in fewer resources dedicated to data security operations, ubiquitous compliance controls, and significantly reduced risk across your business.

The platform offers capabilities for discovering, protecting and controlling access to databases and files—and can secure assets residing in cloud, virtual, big data and physical environments. This scalable, efficient data security platform enables you to address your urgent requirements, and it prepares your organization to nimbly respond 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 protection techniques
  - Transparent encryption for databases and files
  - 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

Encryption or key management environments

- IaaS, PaaS and SaaS: Amazon Web Services, Google Cloud Platform, Microsoft Azure, IBM Cloud, Salesforce, Microsoft Office365
- Suported OSs: Linux, Windows and Unix
- Big data: Hadoop, NoSQL, SAP HANA and Teradata
- Database: IBM DB2, Microsoft SQL Server, MongoDB, MySQL, NoSQL, Oracle, Sybase 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, cloud and big data environments
- Flexibility and extensibility enable fast support of additional use cases
- Hardware Security Modules as the secure root of trust for the platform including 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 simplifies data security administration with 'single pane of glass' 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. Organizations can easily uncover and close privacy gaps, prioritize protection, and make informed decisions about privacy and security mandates before a digital transformation implementation.

Accelerate Time to Compliance. Regulators and auditors require organizations to have control of regulated and sensitive data along with the reports to prove it. CipherTrust Data Security Platform capabilities, such as data discovery and classification, encryption, access control, audit logs, tokenization, and key management support ubiquitous data security and privacy requirements. These controls can be quickly 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 of the needed connectors in response to new data protection requirements.

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 cloud vendor encryption lock-in and ensure the data mobility to efficiently secure data across multiple cloud vendors with centralized, independent encryption key management. Organizations that cannot bring their own encryption can still follow industry best practices by managing keys externally using the CipherTrust Cloud Key Manager. The CipherTrust Cloud Key Manager supports Bring Your Own Key (BYOK) use-cases across multiple cloud infrastructures and SaaS applications. 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 data, wherever it is created, used, or stored.

Featured products:

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

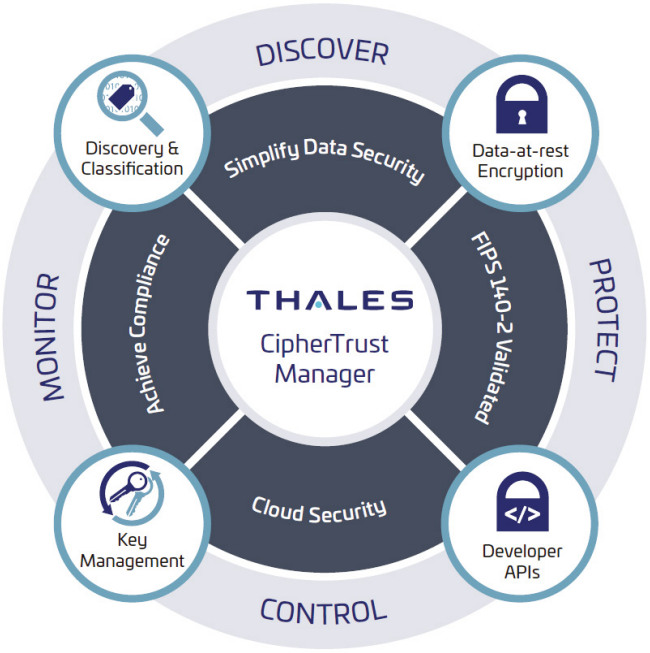
Data Discovery and Classification enables organizations to discover and classify sensitive data from a single pane of glass. Organizations can understand risks, uncover gaps, and make better decisions about both third-party data sharing and cloud migration.

CipherTrust Enterprise Key Management manages encryption keys for many sources and environments across the enterprise, simplifying encryption key management. The CipherTrust KMIP server operates on CipherTrust Manager to centralize key management for many KMIP clients and partner verified solutions. CipherTrust Transparent Data Encryption (TDE) Key Management is available for many popular databases, and the CipherTrust Cloud Key Manager offers cloud bring you own key (BYOK) life cycle management for many Infrastructure-, Platform- and Software as a Service cloud providers.

Data-at-Rest Encryption protects data without requiring any changes to business or data management processes. CipherTrust Transparent Encryption encrypts data across on-premises, cloud, database and big data environments with comprehensive data access controls that can stop the most pernicious attacks. 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 for customer choice based on use-case requirements.

CipherTrust Database Protection solutions protect sensitive database fields without the need for software engineering assistance. The solutions deliver the highest level of separation of duties for access to sensitive data.



CipherTrust Manager

Overview

At the center of the CipherTrust Data Security Platform is CipherTrust Manager, which centralizes keys, management and policies for all CipherTrust Data Security Platform products. Built on an extensible microservices architecture, CipherTrust Manager enables organizations to efficiently address privacy and data protection regulatory mandates and adapt readily as encryption and IT requirements evolve.

CipherTrust Manager simplifies key lifecycle management including activities such as generation, backup and restore, deactivation and deletion. Role-based access to keys and policies, multi-tenancy support, and robust auditing and reporting of key usage and operational changes are additional core features of the product.

CipherTrust Manager is available in both virtual and physical form factors with varying FIPS 140-2 certifications. The virtual appliances can utilize one of several different network-accessible HSM's for a FIPS 140-2 Level 3 root of trust and can be deployed on-premises as well as in private or public cloud infrastructures. This allows organizations to address compliance requirements, regulatory mandates and industry best practices for data security.

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

Benefits

- Centralized key management to allow consolidation of on-premises and cloud encryption keys across multiple applications, data stores, and appliances
- Provides the foundation for the Ciphertrust Data Security Platform, allowing customers the ability to reduce business risk with data discovery, classification and sensitive data protection
- Simplified management with a self-service licensing portal and visibility into licenses available and in use
- Cloud friendly deployment options with support for AWS, Azure, Google Cloud, VMware, OpenStack and more
- Expanded Hardware Security Module (HSM) support for superior key control and generation
- Unparalleled partner ecosystem of integrations with leading enterprise storage, server, database, application and cloud vendors

Key features

- Full Key Lifecycle Management
- 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 integration with SIEM tools.

CipherTrust Manager Technical Specifications

Hardware Specifications (k470, k570)

Chassis Dimensions	19.0"(W) x 21"(D) x 1.75"(H)
Weight	12.7 kg(28lbs)
CPU	Intel Xeon E3-1275v5
Memory	16 GB
Hard Disk and Protections	1 X 2TB SATA SE (Spinning Disk)
Serial Port	1
Ethernet / NICs	4x1GB or 2x10GB/2X1GB
Power Supplies	• Average power (Watts) 0.7A @120V (84W) • Maximum power (Watts) 0.83A @120V (100W) • Voltage: 100-240V 50-60Hz
Power Cord Options	• PSE certified • Multiple country profiles
MTBF Telcordia	153,583
Chassis Intrusion Detection	Tamper seals. k570 Embedded HSM will zero itself upon tamper detection
Operating Temperature	0 to ~35°C
Non-Operating Temperature	-20 to 60 °C
Operating Relative Humidity	5% to 95% non-condensing
FIPS 140-2 Certifications	Luna K7 (https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3205) Luna T7 (https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3898) DPoD (https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3519)
Embedded HSM Administration	k570 (Built in HSM) , Management Console and REST API allow configuration to HSM
Mounting Hardware	• Non-sliding rail hardware and mounts included • Sliding rails available

Software Specifications

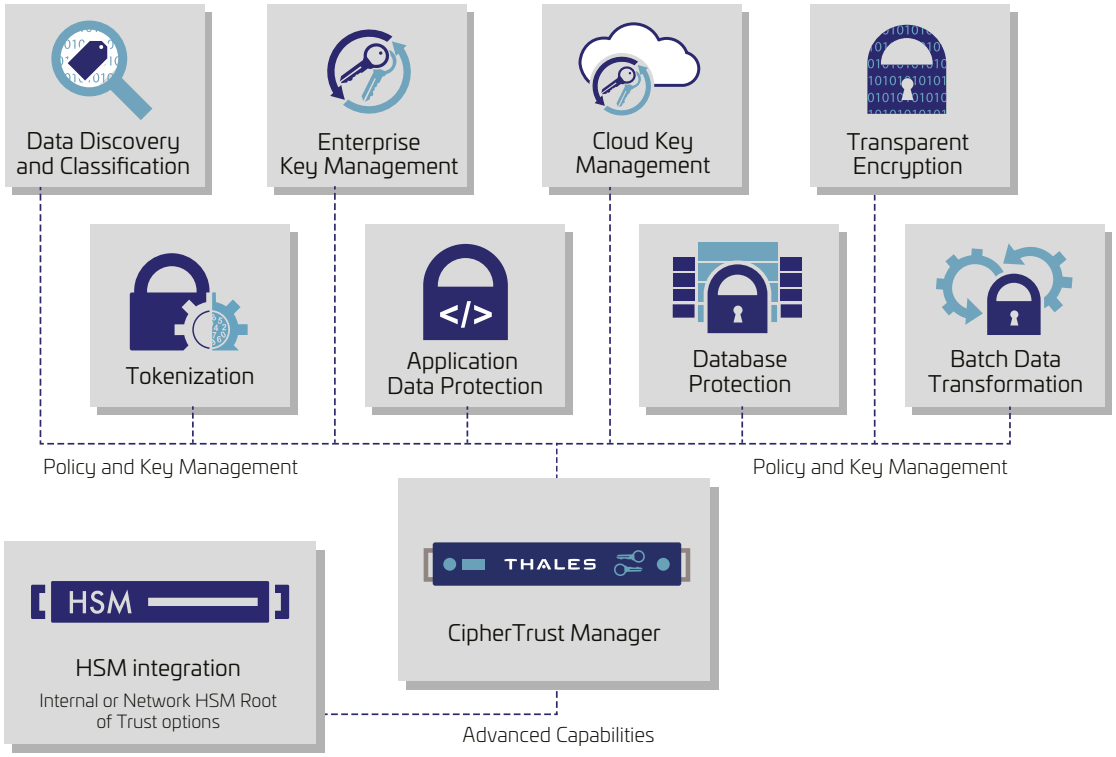
Administrative Interfaces	Management Console, REST API, ksctl (Command Line Interface), NAE XML			
Max Keys	k470 1M	k570 1M	k170v 50K	k470v 1M
Max Domains (multi-tenancy)	1000			
API Support	REST, NAE-XML, KMIP, PKCS#11, JCE, .NET, MCCAPI, MS CNG			
Security Authentication	• Local User • AD/LDAP • Certificate based authentication • K570: Local or Remote PED for master key setup and configuration			
Supported HSMs for Root of Trust	Luna Network HSM, Luna T-Series Network HSM, Luna Cloud HSM, Data Protection on Demand, AWS CloudHSM			
Cluster Support	Active/Active. Max nodes=10 cluster Cluster members can be any model physical/virtual. k170v limited to 2-node clusters			
Backup	Manual and scheduled; option for HSM key to encrypt CM backup			
Network Management	SNMP v1, v2c, v3, NTP, Syslog-TCP			
Syslog Formats	RFC-5424, CEF, LEEF			
Software Certifications and Validations	k570: FIPS 140-2 L3 K470, k170v and k470v can use Luna Network HSM as root of trust for master key			

Specifications for Virtual Machine Deployment

	k170v	k470v
Minimum Number of CPUs	2	4
Minimum RAM (GB)	4	16
Minimum Hard Disk (GB)	100	200
Minimum vNICs	1	2

Unified management and administration across the hybrid enterprise

CipherTrust Manager minimizes capital and expense costs 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. The product also centralizes log collection from connectors that generate logs, such as CipherTrust Transparent Encryption.



Safety Certifications	Applicable Administrative Unit
CB Scheme	44 countries
CSA-UL	Canada/US

Emissions Certifications	
FCC Part 15, Subpart B, Class B	US
EN55032:2010, EN55024:2010,EN61000-3-2:2006 +A1:2009 +A2:2009EN61000-3-3:2008	EU
ICES-003 Issue 4 February 2004	Canada
C-TickAS/NZS CISPR 22:2009	Australia/NZ
VCCI V-3/2009.04	Japan
KN22, KN24, KC Mark	South Korea
NOM	Mexico
BIS	India

CipherTrust Data Discovery and Classification

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, prioritizing remediation, or securing your cloud transformation and third-party data sharing.

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 Data Discovery and Classification 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.

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

Single pane of glass for clear visibility

Data Discovery and Classification 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, or 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, CCPA, etc., while its flexibility easily handles custom policies based on specific patterns, algorithms and more.

Demonstrate compliance

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

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.)

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

Network Connection

- At least 1GB

CipherTrust Enterprise Key Management

CipherTrust key management products centralize key management for CipherTrust platform as well as commercial off the shelf (COTS) applications. Organizations gain greater command over encryption keys while increasing data security. CipherTrust key management products connect with applications through standard interfaces and deliver access to robust key management and encryption functions.

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, allowing those keys to be managed with a common set of policies. CipherTrust Manager is certified with a number of 3rd party applications and devices that utilize KMIP.

Database and Linux Key Management

CipherTrust Enterprise Key Management solutions for databases and Linux can provide high security while providing enhanced IT efficiency. For both Transparent Data Encryption (TDE) key management and Linux Unified Key Setup (LUKS), an agent on the database or Linux server requests keys from CipherTrust Manager and serves them to TDE or LUKS.

Key Management for Proprietary Applications

For the most convenient integrations into applications that perform encryption but 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 that can be installed on supported application server environments.

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
- Assymetric key algorithms
  - RSA
  - Elliptic Curve: brainpool, prime, secp

Third-Party Encryption
- Microsoft SQL TDE, Oracle TDE, IBM Security Guardium Data Encryption, KMIP-clients
- Example partners: Nutanix, Linoma, NetApp, Cisco, MongoDB, DataStax

API Support
- PKCS#11
- 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 Manager

Many cloud service providers offer data-at-rest encryption capabilities. Meanwhile, many data protection mandates require that encryption keys be managed remote from the cloud service provider. "Bring Your Own Key" (BYOK) services and API's can fulfill these requirements.

Customer key control

BYOK-based customer key control allows for the separation, creation, ownership and control, including revocation, of encryption keys or tenant secrets used to create them. Leveraging BYOK API's, the CipherTrust Cloud Key Manager reduces key management complexity and operational costs by giving customers full lifecycle control of encryption keys with centralized management and visibility.

IT efficiency and compliance tools

The combination of centralized key management for multiple cloud providers in a single browser window, automated key rotation with support for automated refreshing of expired keys, federated login for supported clouds, and management of native cloud keys offers enhanced IT efficiency. CipherTrust Cloud Key Manager cloud-specific logs and prepackaged reports enable fast compliance reporting.

Strong encryption key security

Customer key control requires secure key generation. CipherTrust Cloud Key Manager leverages the security of the CipherTrust Manager to create and store keys.

Implementation choices that match your needs

CipherTrust Cloud Key Manager offers several convenient implementation choices to meet your security and deployment needs:

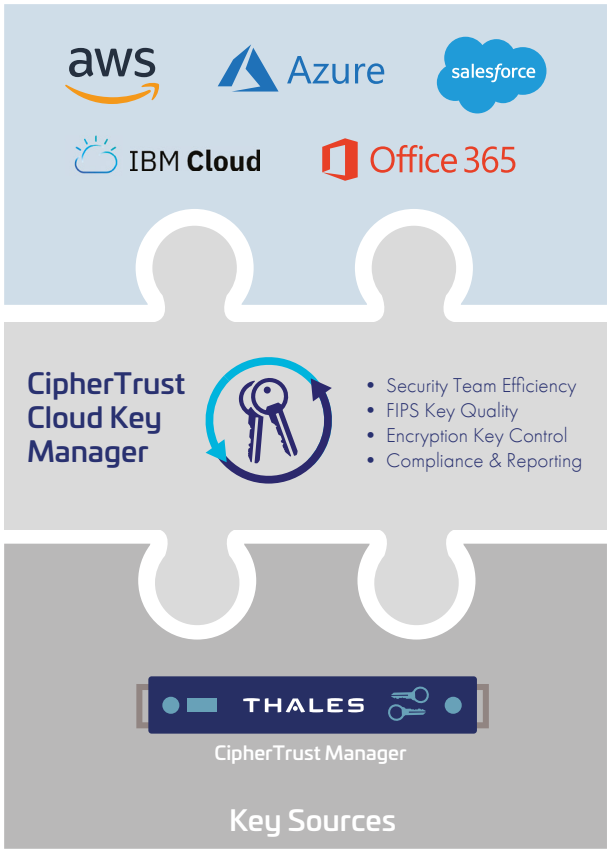
- All-software: The CipherTrust Cloud Key Manager Virtual Appliances and CipherTrust Manager virtual appliances can be instantiated in Amazon Web Services or Microsoft Azure, or deployed in any public- or private cloud leveraging VMware.
- Customers that require FIPS 140-2 Level 3 can deploy or utilize a compliant model of a CipherTrust Manager as a key source for CipherTrust Cloud Key Manager. In addition, the FIPS 140-2 Level 3 certified Thales Luna Network HSM can be deployed as a root of trust for the virtual appliance key sources.

Key benefits

- Leverage the value of "Bring Your Own Key" services with full-lifecycle cloud encryption key management. Lifecycle controls include automated key rotation based on basic or "on expiration" schedules, management of cloud-native keys for supported clouds), and full dynamic key meta-data management.
- Comply with the most stringent data protection mandates with up to FIPS 140-2 Level 3 validated key creation
- Gain higher IT efficiency with centralized key management across multiple cloud environments

Supported cloud environments

- IaaS and PaaS: Microsoft Azure, Azure China National Cloud, Microsoft Azure Stack, Amazon Web Services, IBM Cloud
- SaaS: Microsoft Office365, Salesforce.com, Salesforce Sandbox



CipherTrust Transparent Encryption

CipherTrust Transparent Encryption 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 and uninterrupted even during deployment.

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 controls required without operational or business process changes.

Scalable encryption

CipherTrust Transparent Encryption runs at the file system or volume level on a server, and is available for a broad selection of Windows, Linux and AIX platforms. 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 such modern CPUs, such as Intel AES-NI and IBM POWER9.

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.

Non-intrusive, transparent deployment

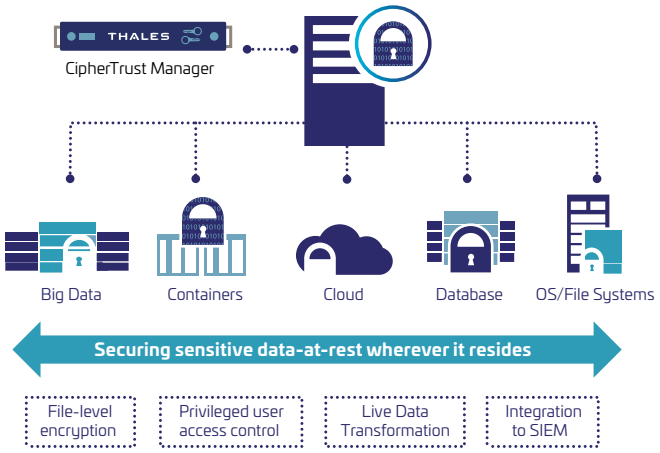
The solution requires no changes to applications, workflows, business or operational procedures.

Key benefits

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

Key features

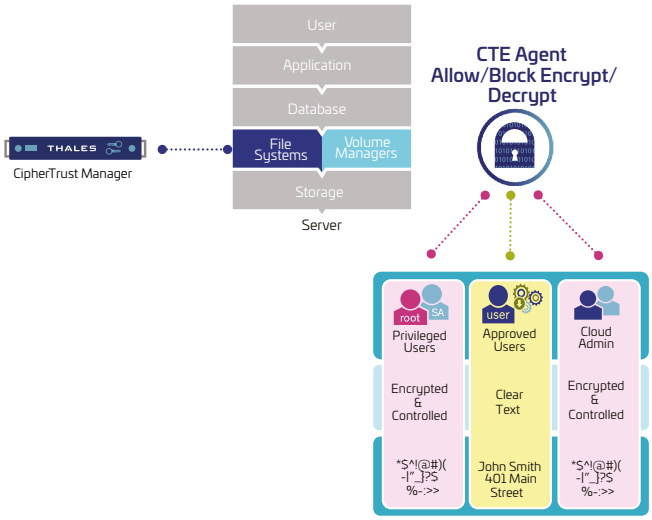
- Broadest platform support in industry: Windows, Linux and AIX operating systems
- High performance encryption: Uses hardware encryption capabilities built into host CPUs - Intel and AMD AES-NI and POWER9 AES encryption
- Logs permitted, denied and restricted access attempts from users, applications 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

Control data with central encryption key and access policy management for on-premises and cloud data, even in hybrid cloud environments. Support for transparent server-based encryption of AWS S3 buckets can help close one of the cloud industry's most common security gaps.



File-level encryption prevents privileged user abuse

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 CipherTrust Transparent Encryption is operating. Information provided also includes actions of security administrators – another item required for compliance audit purposes.

Security Intelligence logs are aggregated by CipherTrust Manager which can then forward them to SIEM system via SYSLOG or CEF among other protocols.

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 Technical Specifications

Encryption Algorithms and Capabilities

- AES, ARIA

Extension Licenses

- Live Data Transformation

Platform Support

- Microsoft: Windows Server 2019, 2016 and 2012
- 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, Sybase 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

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 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.

Live Data Transformation 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.

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

Live Data Transformation Technical Specifications

Operating System Support

- Microsoft: Windows Server 2019, 2016 and 2012
- Linux: Red Hat Enterprise Linux 7 and 8, SuSE Linux Enterprise Server 12 and 15

Cluster support

- Microsoft Cluster: File Cluster, SQL Server Cluster

Database support

- IBM DB2, IBM Informix, Microsoft SQL Server, Oracle, Sybase and others

Big Data Support

- Cassandra, CouchBase, Hadoop, MongoDB, SAP HANA

Backup/Replication Support

- DB2 backup, NetBackup, NetWorker, NTBackup, Oracle Recovery Manager (RMAN), Windows Server Volume Shadow Copy Service (VSS)

CipherTrust Transparent Encryption for SAP HANA

The CipherTrust Transparent Encryption edition for SAP HANA offers a proven approach to safeguarding SAP HANA data that meets rigorous security, data governance and compliance requirements. The solution requires no changes to SAP HANA or the underlying database or hardware infrastructure. Organizations can encrypt SAP HANA data and log volumes and establish strong governance and separation of duties.

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.

Vaulted Tokenization

CipherTrust Vaulted Tokenization 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.

Vaultless Tokenization Technical Specifications

Tokenization capabilities:

- Format-preserving tokens with irreversible option
- Random tokens data length up to 128K
- Date tokenization
- 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 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
- Cryptographic hash functions, including SHA2-256, SHA2-284, SHA2-512, and Base16/Base64
- Regular expressions (Java style)

Supported Token Vault Databases

- Microsoft SQL Server
- Oracle
- MySQL
- Cassandra

Application integration

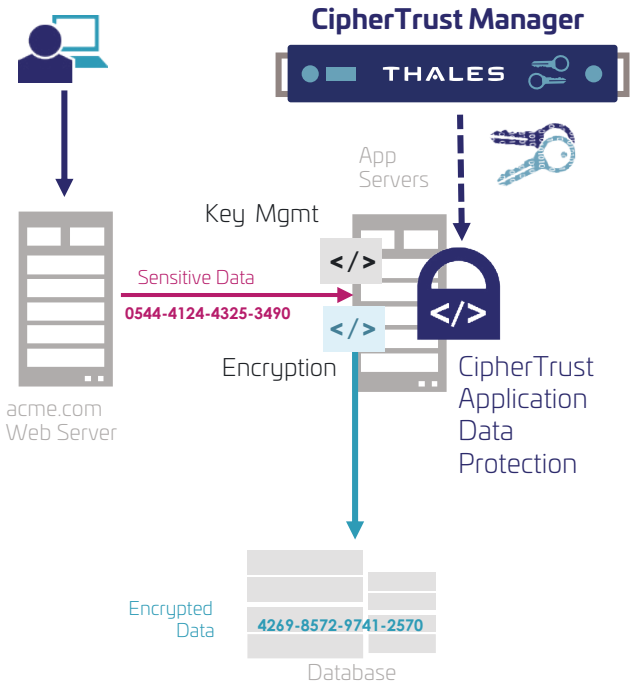
- RESTful APIs
- Java
- .NET

CipherTrust Application Data Protection

Overview

CipherTrust Application Data Protection 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 life cycle state – during transfer, use, backup or copy. CipherTrust Application Data Protection 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.

CipherTrust Application Data Protection 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.



CipherTrust Application Data Protection with Installable Libraries

CipherTrust Application Data Protection 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).

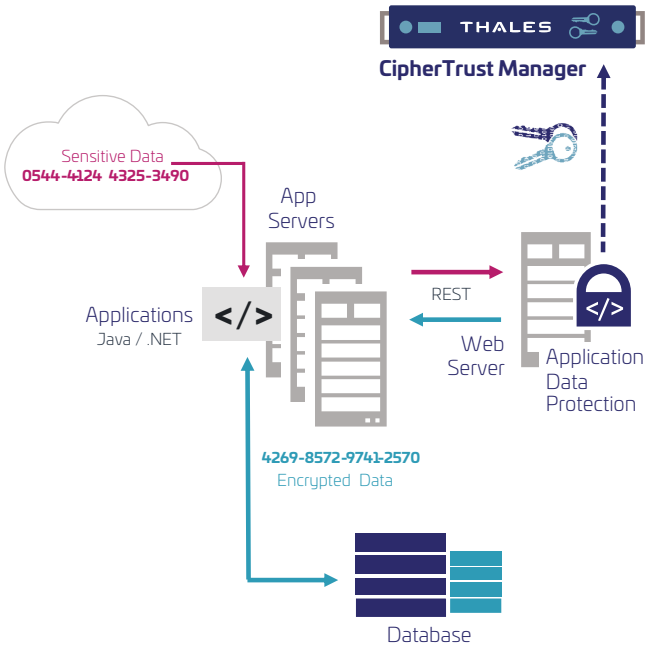
The product supports mulitple core standards: PKCS#11, KMIP, Microsoft Crypto Next Generation (MS-CNG) and Microsoft Cryptographic Service Provider (MS-CSP).

The solution offers encryption flexibility in both development and operations:

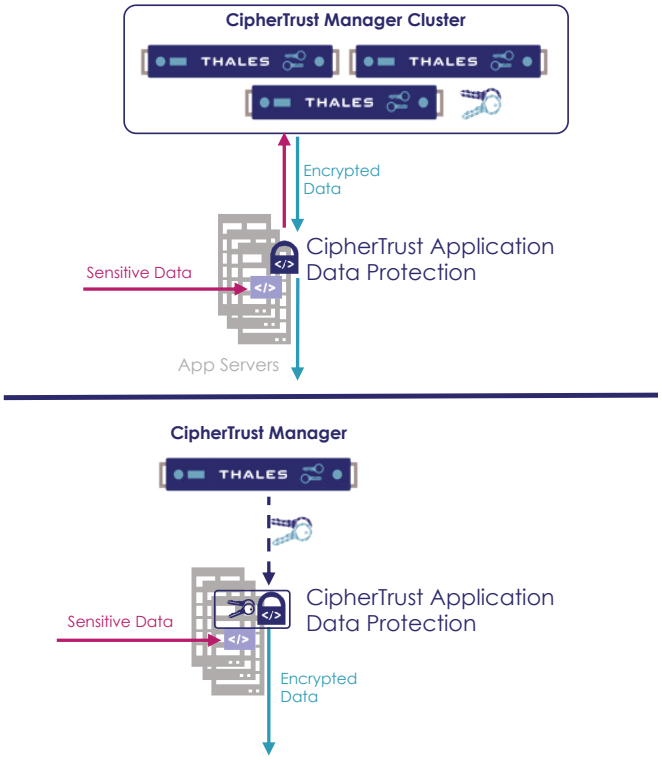
Development flexibility is delivered with a range of architecture and API choices.

- Developers can choose RESTful APIs to limit deployment footprint, leveraging both key management and crypto operations occurring on CipherTrust Manager.
- A wide range of installable development libraries and APIs are available
- Another lightweight deployment option is to install the encryption and key management libraries on a web server and access them from an application server using REST APIs.

Encryption Operational flexibility is delivered by the choice, for the *libraries* or Web Services edition of the product, to encrypt locally or on CipherTrust Manager, without changing any code. The choice is implemented with a simple configuration change.



CipherTrust Application Data Protection installed as a Web Service



Where to encrypt involves choices and potential benefits:

- Encryption on CipherTrust Manager offers security, performance, and scalability benefits, and ensures that keys never leave the trusted CipherTrust Manager for the highest level of security. Offloading encryption from application servers can enable them to perform better. And, embedded in CipherTrust Application Data Protection libraries are load-balancing mechanisms that enable 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.

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

Rich Encryption Ecosystem

CipherTrust Application Data Protection provides key management and/or encryption services for a a formidable ecosystem of solutions including Linux Unified Key Management (LUKS), key management for Transparent Data Encryption (TDE) vendors including Oracle, Microsoft SQL Server, and IBM DB2, among many others.

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/C++, .NET, .Net Core
- XML open interface, KMIP standard
- Web services: REST

Encryption Algorithms

- 3DES, AES, AES-XTS, SHA, HMAC, RSA, 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

Supported Platforms for ICAPI Provider

- Red Hat Enterprise Linux 5.4 and above
- Microsoft Windows 2003, 2008 R2, and 7 in both 32-bit and 64-bit

CipherTrust Database Protection

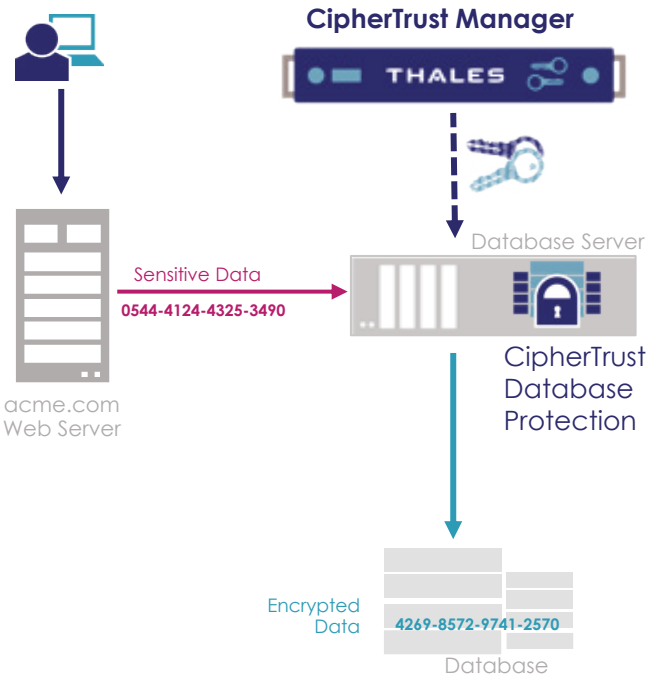
Overview

CipherTrust Database Protection products provide transparent column-level encryption of structured, sensitive data residing in databases, such as credit card, social security numbers, national ID numbers, passwords, and email addresses. CipherTrust Database Protection and CipherTrust Teradata Database Protection offer convenient choices in database protection and both leverage CipherTrust Manager for centralized key management.

The solutions enable sensitive data fields in databases to be efficiently protected and secured. Both solutions are transparent to applications and business processes, requiring no changes. And both are cloud-friendly. For efficiency, both products offer mechanisms either to encrypt locally for performance or in CipherTrust Manager to ensure that encryption keys never leave the secure enclave, without changing any code. The choice is implemented with a simple configuration change.

CipherTrust Database Protection

CipherTrust Database Protection encrypts data, leveraging database views and triggers to ensure that access to non-encrypted and encrypted fields remains transparent to applications. Key granularity is on a per-field basis. Day to day use of the product is preceded by a data migration process involving selection of data to encrypt, database table, view and trigger design, and finally bulk data encryption.



Database Protection Technical Specifications

Supported Databases

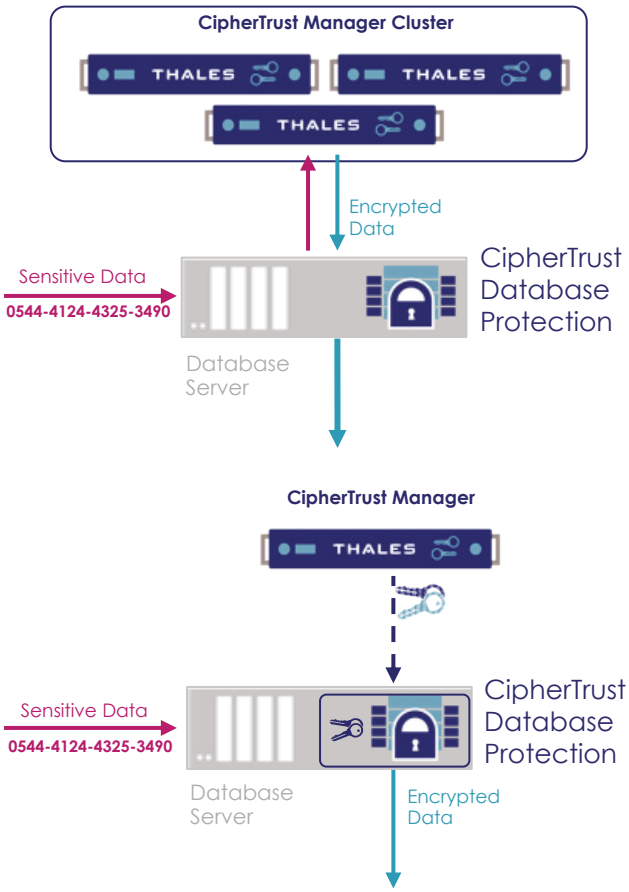
- Oracle
- Microsoft SQL Server
- IBM DB2
- Teradata Database

Supported Platforms

- Microsoft Windows
- Linux
- Solaris
- HP-UX
- AIX

Encryption Algorithms

- AES, 3DES, FF3, FF1, RSA, ECC



Where to encrypt involves choices and potential benefits:

- Encryption on CipherTrust Manager offers security, performance, and scalability benefits, and ensures that keys never leave the trusted CipherTrust Manager for the highest level of security. Offloading encryption from database servers can enable them to perform better. And, embedded in CipherTrust Database Protection are load-balancing mechanisms that enable encryption load to be spread across a cluster of CipherTrust Managers.
- Encryption on the database server can provide potentially higher performance for certain fields of database encryption. 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.

CipherTrust Teradata Database Protection

CipherTrust Teradata Database Protection encrypts or tokenizes data in-place with key granularity on a per-field basis, with convenient blacklist and whitelist access control for fast implementations. Finally, during decryption operations, field masking may be configured on a per-user basis.

Benefits

- Centralized key management for multiple on-premises data stores and cloud infrastructures
- Simplified management with self-service licensing portal and visibility into licenses in use
- Cloud friendly deployment options with support for AWS, Azure, Google Cloud, VMware and more

Teradata Database Protection Technical Specifications

Supported Databases
- Teradata Database, minimum version 14.0

Supported Platforms
- SUSE Linux Enterprise Server (SLES) minimum version 10

Encryption Algorithms
- AES, FF1, FF3

Maximum Column Widths
- ASCII—16KB, Unicode—8KB

Encryption Controls
- Blacklist/whitelist access
- Identity-based access per column
- Dynamic masking based on identity

CipherTrust Batch Data Transformation

CipherTrust Batch Data Transformation provides static data masking services that enable secure, fast and efficient use of modern digital transformation initiatives such as data warehouses, big data on premises and in the cloud, sharing databases with DevOps, and outsourced data analysis.

Flexible data masking

CipherTrust Batch Data Transformation leverages both CipherTrust Application Data Protection and CipherTrust Tokenization. Batch Data Transformation utilizes CipherTrust Application Data Protection for encryption and key management and communicates with the CipherTrust Tokenization Server for tokenization services.

Data security for digital transformation

Transformation options include either encryption or tokenization for files or supported databases.
Use cases include:

- Rapid data rekeying
- Safe database or data extract sharing with big data consumers, DevOps, or third parties
- Preparing data for safe cloud migration
- Preparing a database for tokenization or application-level encryption

Key benefits

- Enables new data uses with flexible security
- Accelerates deployment of CipherTrust Tokenization with Dynamic Data Masking or custom applications based on CipherTrust Application Data Protection
- Leverages and expands existing investments in the CipherTrust Data Security Platform

Technical specifications

Data Transformation Options:

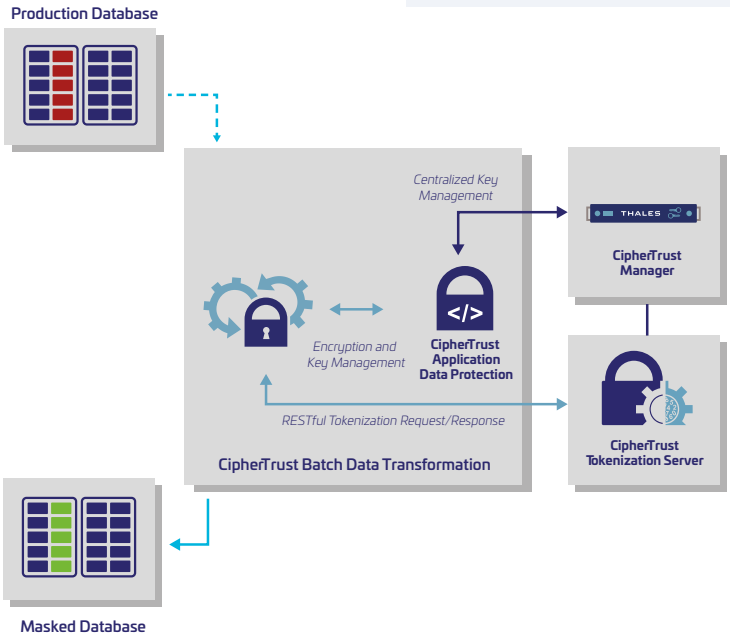
- Tokenization, Data Encryption
- Formatting preserving alpha/numeric

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

Hardware and Operating System Requirements:

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



THALES

Contact us

For all office locations and contact information, please visit
www.thalestct.com/contact-us

> www.thalestct.com <