thalestct.com

THALES
Building a future we can all trust

CipherTrust Data Security Platform Architecture

A technical introduction to the CipherTrust Data Security Platform and Sample Use Cases

White Paper

Contents

Executive Summary

With the widespread adoption of cloud services, big data environments, and IoT technologies, organizations are moving huge amounts of sensitive data rapidly to third party and partner infrastructures. All of this makes today's data environments increasingly complex to manage and secure. So, it comes as no surprise that almost half of the respondents to the Thales 2021 Data Threat Report survey, see multi-cloud data security management as more complex to manage.

The CipherTrust Data Security Platform from Thales integrates data discovery, classification, and industry-leading data protection solutions across diverse IT environments to provide adaptive data-centric security. The platform provides powerful tools to combat external threats, guard against insider abuse, and establish persistent controls, even when data is stored in the cloud or any external provider's infrastructure and supports an evolving regulatory landscape. This white paper provides an overview of the deployment architecture of the CipherTrust Platform products and the compelling use-cases that they enable for customers along their data protection journey.

Platform Capabilities and Benefits

Platform Capabilities

- Centralized management console
- Data discovery and classification
  - Risk analysis with data visualizations
- Data Protection Connectors
  - Transparent encryption for files, databases and containers
  - Application-layer data protection
  - Format preserving encryption
  - Tokenization with static and dynamic data masking
  - Database protection
  - Privileged user access controls
- Proactive Data Protection
  - Integrated data discovery, classification and automated protection
- Centralized enterprise key management
  - FIPS 140-2 compliant
  - Multi-cloud key management
  - Unparalleled ecosystem of KMIP partner integrations
  - Transparent Data encryption (TDE) key management
- Monitoring and reporting

Environments and Technologies Supported

- IaaS, PaaS and SaaS: Amazon Web Services, Google Cloud Platform, Microsoft Azure, IBM Cloud, Salesforce, Microsoft Office365 , Oracle Cloud Infrastructure, Alibaba Cloud
- OS: Linux, Windows and AIX
- Big data: Hadoop, NoSQL, SAP HANA and Teradata
- Databases: IBM DB2, Microsoft SQL Server, MongoDB, MySQL, NoSQL, Oracle, Sybase and others
- Containers: Docker, Red Hat OpenShift
- Any storage environment

Compliance Regulations Supported

GDPR

PCI-DSS

HIPAA

SOX/GLBA

ISO/IEC 27002:2013

FIPS 140-2

FISMA, FedRAMP

NIST 800-53 Rev 4

California Consumer Privacy Act

South Africa POPI Act

Japan My Number Compliance

South Korea's PIPA

India's Aadhaar Act

Philippine's Data Privacy Act

Monitory Act of Singapore

Australia Privacy Amendment

CipherTrust Platform – Products Summary

The CipherTrust Data Security Platform features the following products to discover, classify and protect sensitive data to enable organizations to securely extract value from sensitive data and confidently adopt digital transformation technologies

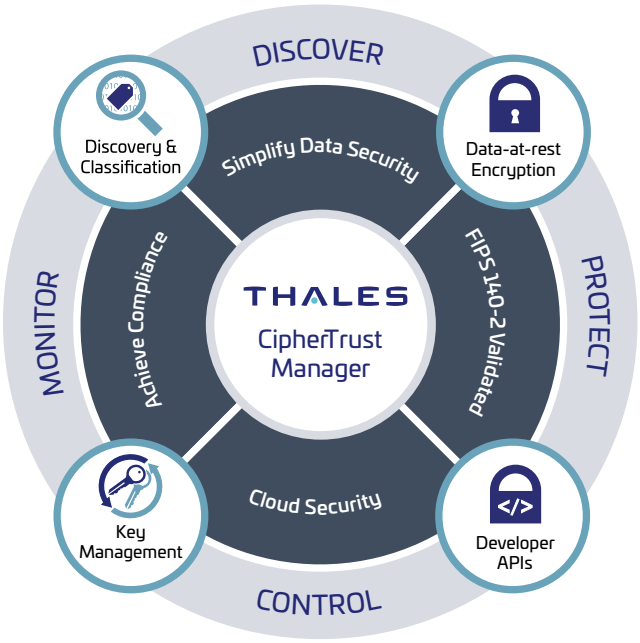

Figure 1: CipherTrust Data Security Platform

- **CipherTrust Manager**
  CipherTrust Manager is the central management point for the platform. It is an industry-leading enterprise key management solution that enables organizations to centrally manage encryption keys, provide granular access controls and configure security policies. CipherTrust Manager manages key lifecycle tasks including generation, rotation, destruction, import and export, provides role-based access control to keys and policies, supports robust auditing and reporting, and offers development- and management-friendly REST APIs. CipherTrust Manager is available in both virtual and physical form-factors that integrate with FIPS 140 validated Thales TCT Luna T-Series Network hardware security module (HSM) or Luna as a Service cloud-based HSM to securely store master keys with the highest root of trust.
- **CipherTrust Data Discovery and Classi ication**
  CipherTrust Data Discovery and Classification locates regulated data, both structured and unstructured, across the cloud, big data, and traditional data stores. A single pane of glass delivers understanding of sensitive data and its risks, enabling better decisions about closing security gaps, compliance violations, and prioritizing remediation. The solution provides a streamlined workflow all the way from policy configuration, discovery, and classification, to risk analysis and reporting, helping to eliminate security blind spots and complexities.
- **CipherTrust Transparent Encryption**
  CipherTrust Transparent Encryption delivers data-at-rest encryption, privileged user access controls and detailed data access audit logging. Agents protect data in files, volumes and databases on Windows, AIX and Linux OS's across physical and virtual servers and in cloud and big data environments. The Live Data Transformation extension is available for CipherTrust Transparent Encryption, providing zero-downtime encryption and data rekeying. In addition, security intelligence logs and reports streamline compliance reporting and speed up threat detection using leading security information and event management (SIEM) systems.
- **CipherTrust Intelligent Protection**
  CipherTrust Intelligent Protection enables organizations to rapidly discover and classify data based on sensitivity, vulnerability, and other risk profiles and pro-actively protect at-risk data using encryption and access controls. It integrates CipherTrust Data Discovery with Classification and CipherTrust Transparent Encryption to improve operational efficiencies, accelerate time to compliance, and pro-actively close security gaps.

- **CipherTrust Application Data Protection**
  CipherTrust Application Data Protection delivers crypto functions such as key management, signing, hashing and encryption services through APIs, so that developers can easily secure data at the application server or big data node. The solution comes with supported sample code so that developers can move quickly to securing data processed in their applications. CipherTrust Application Data Protection accelerates development of customized data security solutions, while removing the complexity of key management from developer responsibility and control. In addition, it enforces strong separation of duties through key management policies that are managed only by security operations.
- **CipherTrust Tokenization**
  CipherTrust Tokenization is offered both vaulted and vaultless tokenization and can help reduce the cost and complexity of complying with data security mandates such as PCI-DSS. The vaultless offering includes policy-based dynamic data masking. Tokenization replaces sensitive data with a representative token, so that the sensitize data is kept separate and secure from the database and unauthorized users and systems. Both offerings make it easy to add tokenization to applications.
- **CipherTrust Database Protection**
  CipherTrust Database Protection solutions integrate data encryption for sensitive fields in databases with secure, centralized key management and without the need to alter database applications. CipherTrust Database Protection solutions support Oracle, Microsoft SQL Server, IBM DB2 and Teradata databases.
- **CipherTrust Key Management**
  CipherTrust Key Management delivers a robust, standards-based solutions for managing encryption keys across the enterprise. It simplifies administrative challenges around encryption key management to ensure that keys are secure and always provisioned to authorized encryption services. CipherTrust Key Management solutions support a variety of use cases including:
  - **CipherTrust Cloud Key Manager** streamlines bring your own key (BYOK) management for Amazon Web Services, Microsoft Azure, Salesforce and IBM Cloud. The solution provides comprehensive cloud key lifecycle management and automation to enhance security team efficiency and simplify cloud key management.
  - **CipherTrust TDE Key Management** supports a broad range of database solutions such as Oracle, Microsoft SQL, and Microsoft Always Encrypted.
  - **CipherTrust KMIP Server** centralizes management of KMIP clients, such as full disk encryption (FDE), big data, IBM DB2, tape archives, VMware vSphere and vSAN encryption, etc.

CipherTrust Platform Connectors

CipherTrust Manager

CipherTrust Manager enables organizations to centrally manage encryption keys, provide granular access control and configure security policies. It manages key lifecycle tasks including generation, rotation, destruction, import and export, provides role-based access control to keys and policies, supports robust auditing and reporting, and offers developer friendly APIs.

- **Unified Management Console**
  CipherTrust Manager provides a single pane of glass for discovering and classifying sensitive data integrated with a comprehensive set of data protection connectors to encrypt or tokenize data to reduce business risk and satisfy compliance regulations. It streamlines provisioning of connector licenses through a new customer facing licensing portal and provides better visibility and control of licenses in use.
- **Centralized Key Management and Access Control**
  It offers centralized key lifecycle, certificate and policy management with role-based access control and provides full audit log review. It authenticates and authorizes administrators and key users using existing AD and LDAP credentials.
- **Cloud Friendly Deployment Options**
  CipherTrust Manager offers several options to securely migrate applications to multiple cloud environments. It offers support for AWS, Azure, Google Cloud, VMware, HyperV, Oracle VM and more. In addition, CipherTrust Cloud Key Manager supports bring your own key (BYOK) across multiple cloud infrastructures and SaaS applications.
- **Developer Friendly APIs**
  CipherTrust Manager offers new REST interfaces, in addition to KMIP and NAE-XML APIs, for developers to simplify deployment of applications integrated with key management capabilities and automate development and testing of administrative functions
- **Improved Monitoring and Alerting**
  It includes tracking of all administrator access, encryption key state and policy changes in multiple log formats (RFC-5424, CEF, and LEEF) for easy integration with SIEM tools. In addition, customers can generate pre-configured and customizable email alerts (SNMP v1, v2c, v3).
- **Hybrid High-Availability Clustering**
  It offers a choice of clustering CipherTrust Manager physical appliances (k470, k570) and a virtual appliances (k170v, k470v) for high-availability environments to ensure optimum processing regardless of the workload location (data center or cloud).

- **Robust Separation of Duties and Multitenancy Support**
  CipherTrust Manager can enforce strong separation of duties by requiring the assignment of key and policy management privileges to one or more data security administrators for different departments within a large enterprise. It provides capabilities to create multiple domains to support large enterprises with distributed locations.
- **FIPS 140-2 Compliant**
  CipherTrust Manager provides several options to integrate with a FIPS 140 validated physical or virtual HSMs as a secure root of trust for better key entropy.
- Built-in HSM crypto accelerator card on a CipherTrust Manager k570 appliance.
- Network attached Luna HSM with HA clustering
- Luna as a Service, Luna Cloud HSM on Data Protection on Demand and other cloud HSMs like AWS CloudHSM, Azure Dedicated HSM, and IBM Cloud HSM.

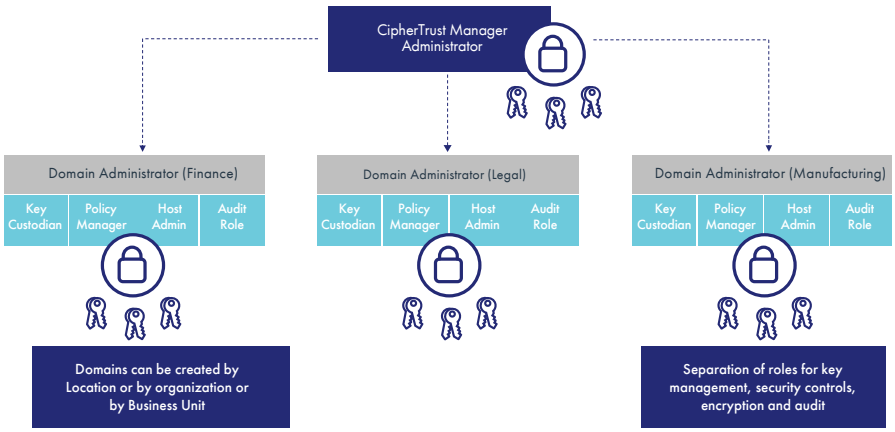

Figure 2: Multi-Tenancy Support with Strong Separation of Duties

CipherTrust Enterprise Key Management

CipherTrust Enterprise Key Management solutions enable organizations to centrally manage and store cryptographic keys and policies for third party devices including Microsoft SQL TDE, Oracle TDE, and KMIP-compliant encryption products. CipherTrust Enterprise Key Management delivers a robust, standards-based platform for managing encryption keys from disparate devices across the enterprise. It simplifies the administrative challenges around encryption key management to ensure that keys are secure and always provisioned to authorized encryption services.

- **CipherTrust Cloud Key Manager** simplifies Bring Your Own Keys (BYOK) and provider created keys for multiple cloud service providers and SaaS applications, while addressing enterprise needs to meet compliance and best practices for managing encryption key life cycles outside of their native environments, without the need for enterprises to become cryptographic experts. It uses CipherTrust Manager as the key source
- **CipherTrust KMIP Server** supports interoperability with a broad range of KMIP compatible data storage devices including SAN and NAS storage arrays, self encrypting drives and hyper-converged infrastructure solutions and follow best practices for strong and secure enterprise key management. CipherTrust Manager has already been certified with a number of 3rd party applications utilizing KMIP.
- **CipherTrust TDE Key Management** provides key lifecycle management for Oracle TDE master encryption keys and Microsoft SQL Server database encryption keys to meet compliance requirements and follow best practices.
- **CipherTrust LUKS Key Management** provides transparent disk encryption for Linux. The LUKS Key Agents enables you to centrally manage encryption keys for Linux disk partitions.

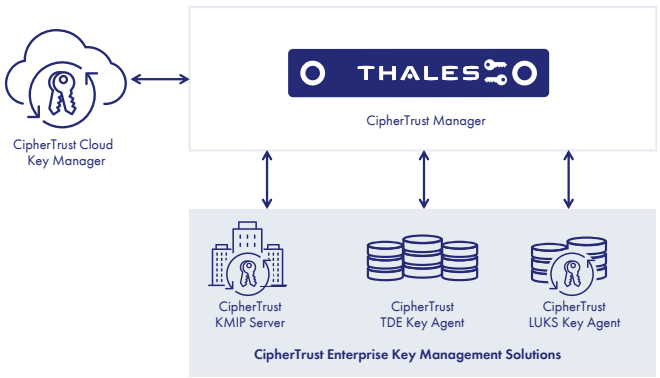

Figure 3: CipherTrust Enterprise Key Management Solutions

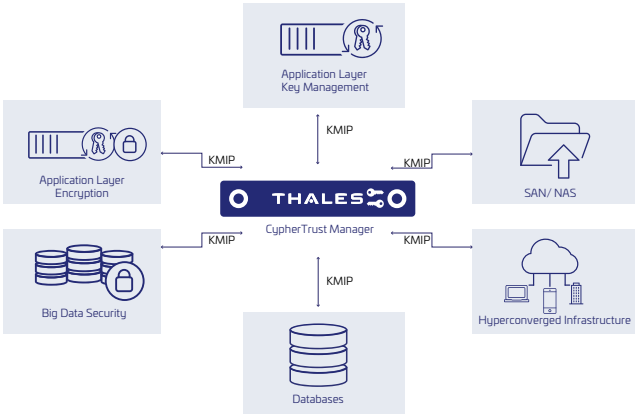

Figure 4: KMIP Client Types Supported by CipherTrust Manager

CipherTrust KMIP Server

CipherTrust Manager offers comprehensive support for the KMIP standard. Effectively, any device or client software that is KMIP enabled can communicate with CipherTrust Manager to facilitate management of encryption keys. Examples of KMIP clients include management systems in hyperconverged environments (Nutanix), self-encrypting drives in storage systems (Netapp, Dell, IBM, HPE) and native encryption in next-generation databases and virtualized environments.

How it works:

1. CipherTrust Manager needs to be setup for KMIP support, which entails adding the KMIP clients on the CipherTrust Manager.

2. Trust between the CipherTrust Manager and the KMIP client needs to be established.

3. For a mutually authenticated Transport Layer Security (TLS) connection between KMIP clients and servers, the client needs to be registered with the CipherTrust Manager at which point the certificate for the KMIP client gets created.

CipherTrust TDE Key Management

Managing encryption keys for native Transparent Data Encryption (TDE) solutions presents challenges such as isolating keys from the assets they protect and storing them securely - not only a best practice for key management, but a common industry data protection mandate. CipherTrust TDE Key Management solutions centralize key management for your enterprise and cloud-hosted Microsoft SQL Server and Oracle Database, giving you greater command over the keys while increasing your data security

- **Microsoft SQL Server Transparent Data Encryption**
  CipherTrust key management solutions complement Microsoft native TDE by providing secure storage and management of the keys used in Microsoft's database encryption scheme. Microsoft TDE encrypts the sensitive data in the SQL database using a database encryption key (DEK), and Thales interfaces with Microsoft Extensible Key Management (EKM) to store and manage the DEKs in the FIPS 140-2 compliant CipherTrust Manager.
- **Oracle Database Transparent Data Encryption**
  CipherTrust Manager complements Oracle Database native TDE by centrally storing and managing Oracle Database encryption keys. As a part of the Oracle Advanced Security TDE two-tier key architecture, Oracle Database uses master encryption key (MEKs) to encrypt the database encryption keys (DEKs), which are used to encrypt columns and table spaces within the databases. CipherTrust Enterprise Key Management solutions interface with the Oracle Wallet to protect and manage these MEKs within a secure FIPS-certified boundary.

CipherTrust Cloud Key Manager

CipherTrust Cloud Key Manager provides "Bring Your Own Key" (BYOK) services to enable customers to control the keys used to encrypt their data in multiple cloud service providers. Customer key control allows for the separation, creation, ownership and control, including revocation, of encryption keys or tenant secrets used to create them. Leveraging cloud provider BYOK API's, the CipherTrust Cloud Key Manager reduces key management complexity and operational costs by giving customers lifecycle control of encryption keys with centralized management and visibility.

- **Multi-cloud Key Control:** CipherTrust Cloud Key Manager provides comprehensive key lifecycle management to fulfill requirements for safe, comprehensive key management across multiple cloud providers. It satisfies industry best practices and data security standards that mandate encryption keys to be stored and managed centrally, remotely from the cloud service provider and the associated encryption operations.
- **Enhanced IT Efficiency:** Centralized key management gives you access to each cloud provider from a single browser window, including across multiple accounts or subscriptions. Automated key rotation offers IT efficiency and enhanced data security. For workloads that require it, CipherTrust Cloud Key Manager can request creation of native cloud provider keys and provide full lifecycle management for them.
- **Strong Encryption Key Security:** CipherTrust Cloud Key Manager leverages the security of the virtual or physical CipherTrust Manager appliances, as a key source. It can also use Thales hardware security modules (HSMs) to create keys and store with a highest root of trust.

Supported Cloud Environments:

- Amazon Web Services, AWS GovCloud
- Google Cloud
- Google Workspace
- Microsoft Azure, Azure GovCloud
- Microsoft Office365
- Microsoft Azure Stack
- Oracle Cloud Infrastructure (OCI), Oracle cloud for Government, Oracle US Defense Cloud, Oracle National Security Regions
- IBM Cloud
- Salesforce.com, SalesForce GovCloud Plus
- Salesforce Sandbox

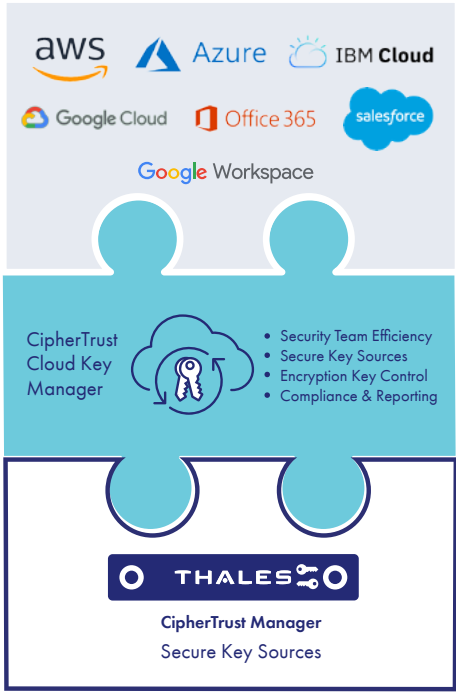

Figure 5: Support for Multiple Cloud Environments

CipherTrust Data Discovery and Classification

CipherTrust Data Discovery and Classification enables organizations to get complete visibility of their sensitive data with efficient data discovery, classification, and risk analysis across cloud, big data, and traditional environments. It enables organizations to uncover and mitigate data privacy gaps and proactively respond to growing data privacy and security regulations, such as GDPR, CCPA, PCI DSS, HIPAA and more.

CipherTrust Data Security Platform unifies data discovery, classification and data protection, as well as granular access controls and centralized key management – all on a single platform. CipherTrust Data Discovery and Classification enables IT organizations to manage data privacy and security with centralized management. From a single pane of glass organizations can set policies, discover data that adheres or violates those policies, classify data, and rank risks. They can then automate remediation using CipherTrust data protection solutions to protect sensitive data and respond to regulatory challenges with a single platform. To achieve this clear view, organizations need to:

1. Define Policies: for data privacy, classification profiles, and scans for multiple data stores.

2. Discover: Locate both structured and unstructured sensitive data across the entire enterprise in multi-cloud, big data, relational databases, or file storage systems.

3. Classify: Sensitive data such as national IDs, financial data, and personal data, based on built-in templates or market-proven classification techniques.

4. Analyze Risk: Understand the risks with rich visualizations and risk scores.

5. Remediate: Proactively protect sensitive data soon after it is discovered and classified using risk-based policies

6. Generate Reports: Leverage charts and reports for risk analysis and to support compliance programs.

Figure 6: Streamline Data Discovery, Classification and Remediation Actions

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
  - PostgreSQL
  - SAP HANA
  - Mongo DB
  - MySQL
- Big Data
  - Hadoop Clusters
  - Teradata
- Cloud
  - AWS S3 buckets
  - Azure Blob
  - Azure Table
  - Google Apps (Gmail and Gdrive)
  - Office 365 (Exchange, SharePoint)

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.)

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

Pre-built templates

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

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

CipherTrust Transparent Encryption

CipherTrust Transparent Encryption delivers data-at-rest encryption with centralized key management, privileged user access control and detailed data access audit logging. It transparently encrypts data wherever it resides -- on-premises file systems/servers, across multiple clouds and within big data, and container environments.

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

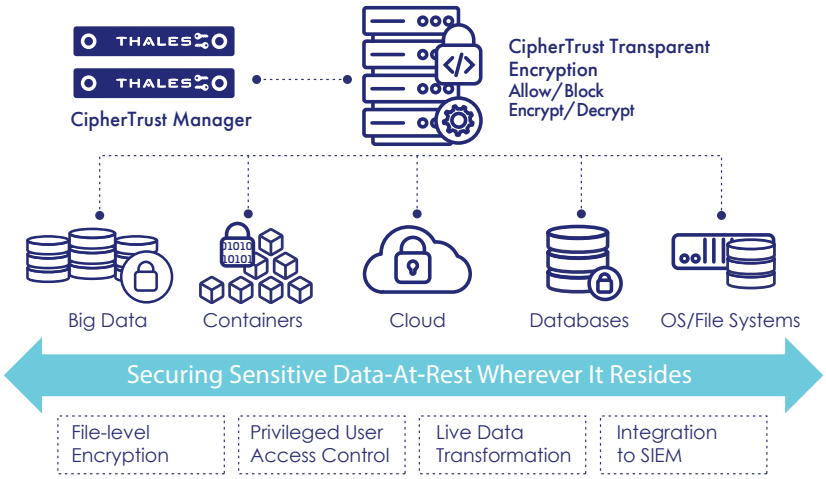

Figure 7: CipherTrust Transparent Encryption

Transparent Encryption agents are kernel level drivers that sit above file systems or volumes in the OS stack. Agents perform policy-based access control, encryption/ decryption and data access auditing. The solution enables organizations to define access policies that are checked before granting access to "GuardPoints" - resources that are protected by fine-grained access policies as follows.

- A GuardPoint can encompass a complete disk drive volume, or a specific directory or an AWS S3 bucket under which all the unstructured files or structured database files reside.
- An access policy defines WHO (user) or WHAT (process) can access the GuardPoint, WHEN, specific file ACTION permitted (read/write/delete/rename) and EFFECT (permit/deny, apply key for encryption/decryption, and audit user access).

Protection Against Privileged User Abuse

Fine-grained access control policies can be setup to restrict privileged users (root, domain admins) to perform administrative tasks only (such as system backups, updates, and hardware maintenance), without giving them access to decrypt sensitive data. Any malware that covertly elevates privileges to gain admin access and gain access to sensitive data is prevented from doing so if access policies are setup correctly.

Preventing Ransomware from Encrypting Sensitive Files

Access policies can be defined to create a whitelist of "trusted" applications to prevent any untrusted binaries (e.g. ransomware) from accessing data stores (GuardPoints) protected by the Transparent Encryption agent and to prevent privileged users from accessing user data in files and databases. The granular access policies can enable organizations to 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.

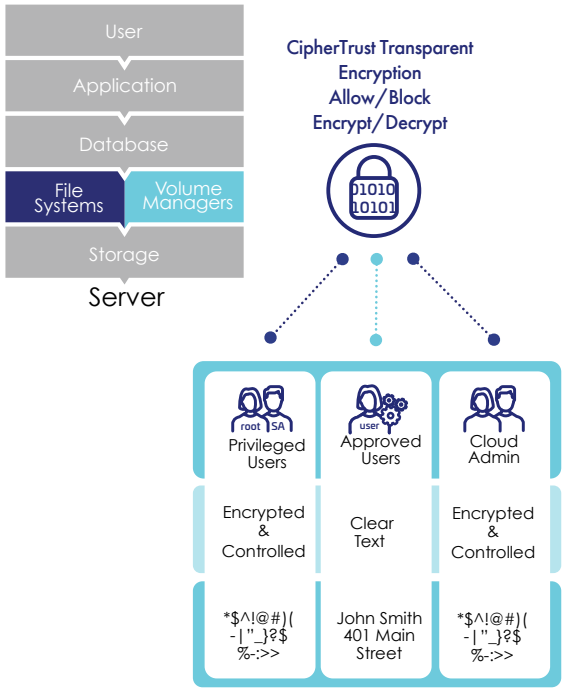

Figure 8: CipherTrust Transparent Encryption Access Control Policies

Integration with SIEM Solutions

CipherTrust security intelligence logs and reports streamline compliance reporting and speed up threat detection using leading security information and event management (SIEM) systems.

CipherTrust Transparent Encryption Extensions

- **Live Data Transformation:** Eliminates the downtime required for initial encryption and scheduled rekeying operations. This patented technology allows for databases or files to be encrypted or re-keyed with a new encryption key while the data is in use without taking applications off-line.
- **SAP HANA Qualified:** SAP has qualified CipherTrust Transparent Encryption with HANA v2.0 to deliver data encryption, key management, privileged user access control, and granular file access audit logs. This solution can be quickly deployed, requiring no changes to SAP HANA or the underlying database or hardware infrastructure.

CipherTrust Application Data Protection

CipherTrust Application Data Protection delivers crypto functions such as key management, signing, hashing and encryption services through APIs so that developers can easily secure data on application servers or big data nodes. The solution comes with supported sample code so that developers can move quickly to securing data processed in their applications. CipherTrust Application Data Protection accelerates development of customized data security solutions, while removing the complexity of key management from the developers' responsibility and control.

Flexible, Efficient Implementation

CipherTrust Application Data Protection reduces the time, complexity, and risk of developing and implementing an in-house encryption and key management solution with support for a range of encryption providers and KMIP. Developers can utilize Java, C and C++ to integrate between applications and CipherTrust Application Data Protection.

Robust Centralized Key Management

Enterprises must not only protect against data theft, but they must also protect their encryption keys from theft, misplacement, or accidental destruction. To facilitate these safeguards, the CipherTrust Application Data Protection crypto library supports enterprise key management through CipherTrust Manager. Depending on a range of architectural, performance and risk assessment choices, customers can choose to retain keys and perform all encryption operations in CipherTrust Manager, similar to an HSM. A configuration change, not requiring any code changes, enables temporary use of keys for encryption or decryption on the CipherTrust Application Data Protection servers. Keys on servers are encrypted when not in use and obfuscated in memory when in use.

Strong Safeguards

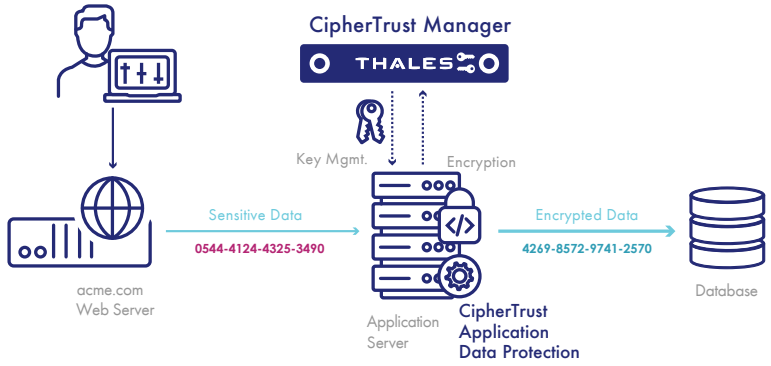

Figure 9: CipherTrust Application Data Protection

CipherTrust Application Data Protection delivers the controls needed to address security policies and compliance mandates, both for data on premises and in PaaS environments. With the solution, you can stop malicious DBAs, cloud administrators, hackers and, in cloud environments, even authorities with subpoenas from accessing valuable data.

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 Tokenization

CipherTrust Tokenization enables organizations to mask sensitive data and address their compliance objectives, while gaining breakthroughs in operational efficiency. It provides a single platform that offers database tokenization and dynamic display security. With this solution, security teams can meet PCI DSS requirements and secure data in cloud, big data, and data center environments—and do so with minimal disruption and administrative overhead. Any organization can replace sensitive assets with tokens, so attackers and malicious contractors and employees can't exploit the information to further their agendas.

Dynamic Data Masking

Security administrators can establish policies to return an entire field tokenized or dynamically mask parts of a field, enabling role-based display security. Administrators can establish settings to have an entire field tokenized or may dynamically mask data so that only portions of a field are visible, such as the first few digits of a Social Security Number or credit card. It can be integrated with your existing LDAP and Active Directory based identity and access management systems, so your security teams can efficiently set granular policies for specific users and groups. For example, a user with customer service representative credentials can see a credit card number with the last four digits visible for customer identification purposes, while a customer service supervisor may be able to see the entire credit card number.

- **Comprehensive Support:** CipherTrust Tokenization supports the following options:
  - Format preserving tokenization
  - Random and sequential tokens

- Either irreversible tokens or the option to delete tokens
- Single and multi-use tokens
- Partial tokenization
- Dynamic data masking, alpha-numeric, and custom mask characters.

- **Efficient Implementation:** This solution offers easy-to-use REST APIs for integration with the CipherTrust Tokenization Server, so application developers can simply and quickly add tokenization and dynamic data masking to applications. Developers don't have to manually institute identity management or redaction policies.
- **Agility and Scalability:** CipherTrust Tokenization delivers the high performance needed to address the operational demands of the most processing-intensive environments. It runs on virtual machines and can be quickly and efficiently scaled up and scaled down to accommodate changing workloads.

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

CipherTrust Database Protection

CipherTrust Database Protection provides 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. This solution enables large amounts of sensitive data to be moved in and out of data stores by efficiently encrypting and decrypting specific columns in databases. No changes are required to applications. It can scale-up to support multiple data centers in on-premises, virtual, and public cloud environments.

CipherTrust Database Protection solutions work with CipherTrust Manager for centralized key and policy management.

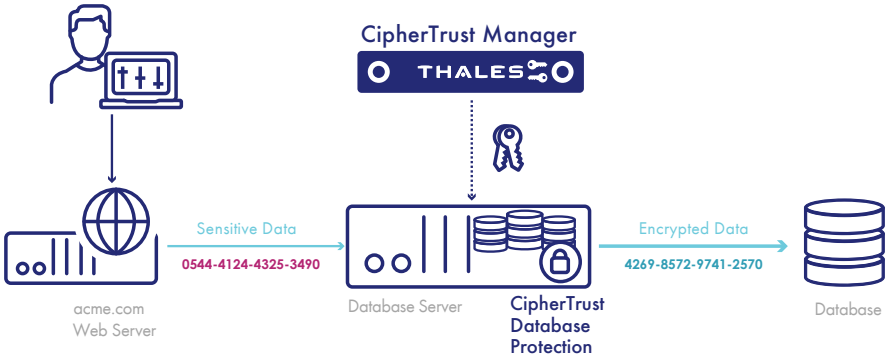

Figure 10: CipherTrust Database Protection

This solution enables organizations to seamlessly encrypt or tokenize sensitive database columns.

Technical Specifications

Supported Databases:

- Oracle
- Microsoft SQL Server
- IBM DB2

Supported Platforms:

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

Encryption Algorithms:

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

Cloud and Virtual Infrastructures:

- Works with all major cloud platforms, including AWS, Microsoft Azure, and VMware

The CipherTrust Platform also offers the following database protection solutions.

CipherTrust Protection for Teradata Database

Delivers fast, efficient and robust data-at-rest security capabilities for Teradata environments, securing sensitive assets in both Teradata Database and the Teradata Integrated Big Data Platform. It integrates with Teradata with simple user-defined functions (UDF) for encryption and decryption. Both Cipher-Block Chaining (CBC) and format-preserving encryption (FPE) modes are available. Use of FPE enables dynamic data masking for decryption operations on a per-user basis. Teradata database and big data analytics solutions enable organizations to more fully leverage information to fuel improved decisions, products, services and business results.

Static Data Masking with CipherTrust Batch Data Transformation

CipherTrust Batch Data Transformation is a high-speed data protection tool offering both encryption and tokenization with static data masking. It leverages CipherTrust Manager for key management and CipherTrust Application Data Protection and CipherTrust Tokenization to facilitate the encryption or tokenization of high volumes of sensitive records without lengthy maintenance windows and downtime. This solution can either encrypt or tokenize sensitive data on a per-column basis. Tokenization and encryption may be used concurrently on different database columns.

Batch Data Transformation is commonly used for a wide range of static data masking use cases:

- Fast and efficient re-keying of existing encrypted data.
- Masking sensitive data before or loading into a data warehouse or data lake.
- Initial encryption or tokenization of existing data in production databases prior to deployment of applications that encrypt or tokenize new data.
- Enable third-party data analysis and clean-up without exposing sensitive or private information
- Enable data science or data analysis team members to utilize accurately represented data without exposure of sensitive content

CipherTrust Data Security Platform Sample Use Cases

Centralized Key Management – Enterprise and Cloud Key Management

The Challenge

The increased adoption of encryption solutions has improved security for enterprises, but it has made life much more challenging for the IT security team, now tasked with managing a variety of cryptographic keys. Nearly all offline data storage devices and many database management systems (DBMS) include the option of embedded native encryption capability. A challenge with these islands of encryption is that keys and key management software from each provider don't usually interoperate well with one another. The resulting silos of security, where system administrators and database administrators (DBAs) have to become the managers of the encryption keys for a particular system, distracts them from their primary tasks of IT and database administration. Along with the resource inefficiency of such a methodology, it also puts an enterprise's overall security posture at risk.

Without a centralized encryption key management solution, security administrators are faced with a costly, inefficient and often impossible task managing disparate encryption keys for many different databases accumulated over time from separate vendors, according to this Aberdeen Report. This heterogeneous world means that an enterprise looking to secure databases, such as Oracle and Microsoft SQL Server using native TDE, has to factor in the increased costs and administrative resources required for managing multiple, incompatible encryption solutions. In addition, each separate encryption system requires specialized training to learn the unique processes that are specific to that system.

When each system administrator separately controls encryption keys for each data repository they manage, the keys are generally stored in the same location as encrypted data, it leaves room for security compromises – the electronic equivalent of taping the key to the front door. Manual systems to store and transmit the encryption keys, lack of password control and the failure to revoke keys when an employee leaves the company can result in data breaches waiting to happen. And strict adherence to compliance requirements is nearly impossible in this situation.

Solution: CipherTrust Enterprise Key Management

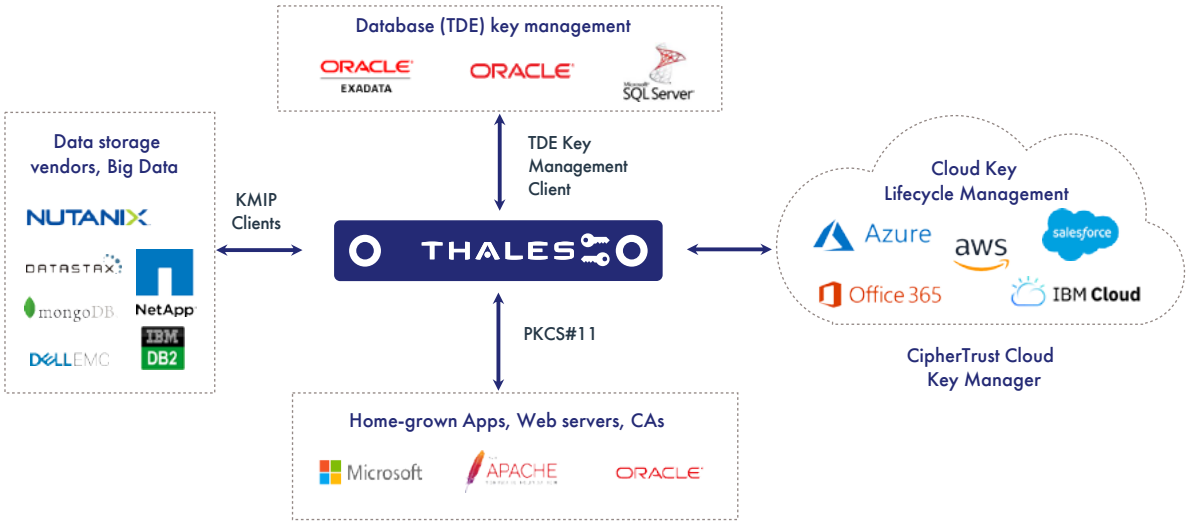

Figure 11: CipherTrust Enterprise Key Management Solutions

CipherTrust Enterprise Key Management solutions centralize key management for internal as well as commercial off the shelf (COTS) applications and storage solutions. This gives customers greater command over your keys while increasing encryption data security. CipherTrust Key Management products connect with your applications through standard interfaces and deliver access to robust key management and encryption functions.

CipherTrust Manager- the foundation for Thales enterprise key management solutions, is a high-availability appliance that centralizes encryption key management for the CipherTrust Data Security Platform and third-party encryption solutions. CipherTrust Manager helps direct key life-cycle tasks including generation, rotation, destruction, import and export as well as provide abilities to manage certificates and secrets. CipherTrust Manager enhances key management by delivering strong separation of duties for increased security.

It supports the following three major interoperability standards that are supported by most server, storage and device vendors currently deployed in existing IT environments.

- **PKCS#11** – Public Key Cryptographic Standard #11 specifies an API for devices to interoperate with hardware security modules (HSM) and smart cards, which hold cryptographic tokens. It is also used to access signing keys from Certification Authorities (CAs) or to enroll user certificates for digital signing and encryption using asymmetric keys.
- **EKM/MSCAPI** – Extensible Key Management (EKM) using the Microsoft Cryptographic APIs (MSCAPI), enables MS SQL Server to communicate with third-party key management servers. The keys must be exported from a provider before they are stored in the database. This approach enables key management that includes an encryption key hierarchy and key backup for Microsoft SQL Server Transparent Data Encryption (TDE).
- **OASIS KMIP** – Key Management Interoperability Protocol (KMIP), defines the standard protocol for any key management server to communicate with clients (e.g. storage devices, databases) that utilize the keys for embedded encryption. KMIP improves interoperability for key lifecycle management between encryption systems and enterprise applications.
- **CipherTrust Cloud Key Manager:** supports bring your own keys (BYOK) and provider created keys for multiple cloud service providers and SaaS applications, while addressing enterprise needs to meet compliance and best practices for managing encryption key life cycles outside of their native environments, without the need for enterprises to become cryptographic experts. It uses CipherTrust Manager as the key source.

Securely Migrating Data to Hybrid Cloud Environments

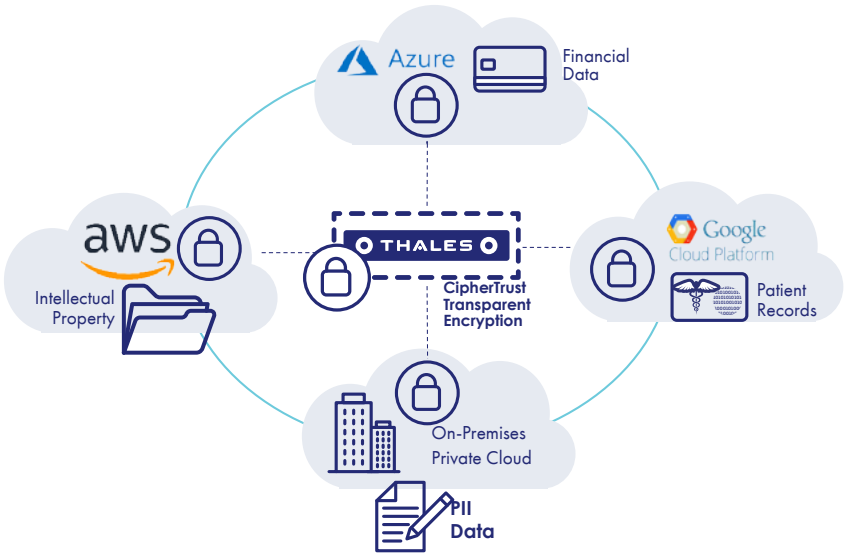

Figure 12: Support for Hybrid Clouds with CipherTrust Transparent Encryption

The Challenge

Cloud computing is transforming the way enterprises, government agencies, and small businesses manage their company data. Elastic public cloud services are enabling agile, cost-effective methods to run business-critical applications and store information. And, while some enterprises aren't yet ready to let go of the traditional on-premises data center, they are exploring and evaluating all available options.

Bring your own encryption (BYOE) is a security model that gives cloud customers complete control over the encryption of their data by allowing them to deploy a virtualized instance of their own encryption software in tandem with the application they are hosting in the cloud. It is possible in this scenario for the end user to manage their encryption keys within the cloud; however, given the legal pressures that a cloud service provider (CSP) could potentially face, it would make little sense to encrypt data and then store the encryption keys in the same environment. To fully secure data in an untrusted and multi-tenant cloud environment, organizations must maintain complete governance and control of their data.

Solution: CipherTrust Transparent Encryption

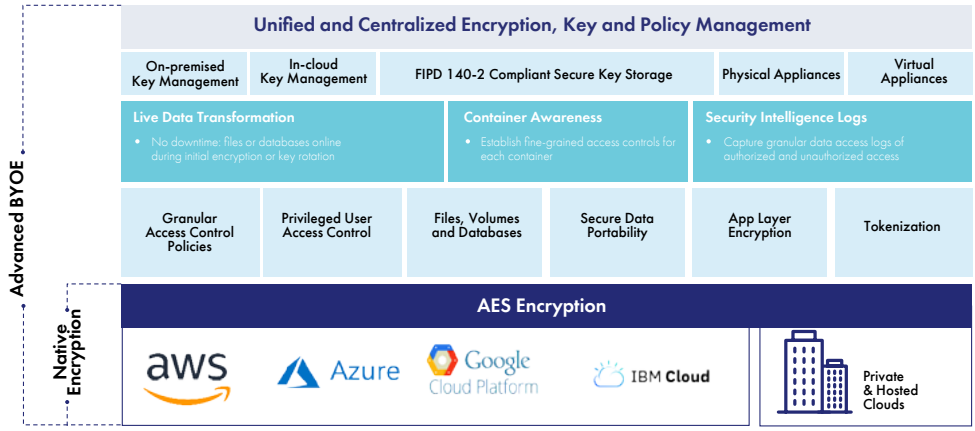

Figure 13: Centralized Encryption, Key and Policy Management with CipherTrust Transparent Encryption

Most cloud service and leading encryption providers use the same encryption technique - Advanced Encryption Standard, or AES. However, encrypting data is only a starting point. To truly protect your data you need to consider the threats you're protecting against, managing encryption keys and access controls across multiple cloud providers. Compared to the native encryption solutions available from cloud providers, CipherTrust BYOE solutions gives you higher confidence that your data is secure and that you are in compliance with mandates by delivering the following solutions.

- CipherTrust Transparent Encryption encrypts sensitive data (such as credit card numbers, personal information, logs, passwords, configurations, and more) on servers in a broad range of files, databases, containers, as well as big data implementations in the cloud. It features granular access controls, which ensures only authorized users or processes can view protected data and prevent rogue administrators from impersonating another user who has access to sensitive data.
- CipherTrust Transparent Encryption extensions enable use of data in the cloud during encryption and rekeying operations with patented Live Data Transformation. CipherTrust Transparent Encryption monitors and logs file access to accelerate threat detection.
- Simplified key management across on-premises and multi-cloud deployments by centralizing control on the FIPS 140-2 compliant CipherTrust Manager.

Protecting Big Data Environments

The Challenge

With the explosive growth of data in every aspect of our lives and in enterprises around the world, there is growing demand to derive value from this data and provide business intelligence. Enterprises depend on this intelligence so they can meet their customers' needs in a timely manner and with greater precision. Along with traditional sources of data such as transactional systems and data warehouses, new sources of data, such as those from the "Internet of Things" (click logs, social media interactions and sensors), have emerged. Collectively, these vastly larger information volumes and new assets are known as Big Data. With nearly every enterprise embracing big data environments, and with large numbers of these environments implemented in the cloud, the security of the sensitive data within the data lake, source data environments, and the reports that hold high-value correlated results have become an insistent concern. Unfortunately, many organizations hesitate looking at security – and more specifically, encryption – when it comes to big data solutions because they are concerned about deploying at scale or impeding the analytics tools that make these solutions so valuable in the first place.

Lack of effective access control

Unauthorized access could not only result in financial loss, identity theft, and reputational damage, but could also run your organization afoul of regulatory compliance. Privileged users are granted substantial access to corporate network resources to be able to perform their routine duties. However, if these users are malicious, or if their credentials are stolen, it can lead to a major data breach.

Data privacy violations

Big data comes from multiple sources at a high velocity, volume, variety, and degree of complexity. It is no secret that privacy violations from internationally-originated data is a huge concern for companies that deal with big data.

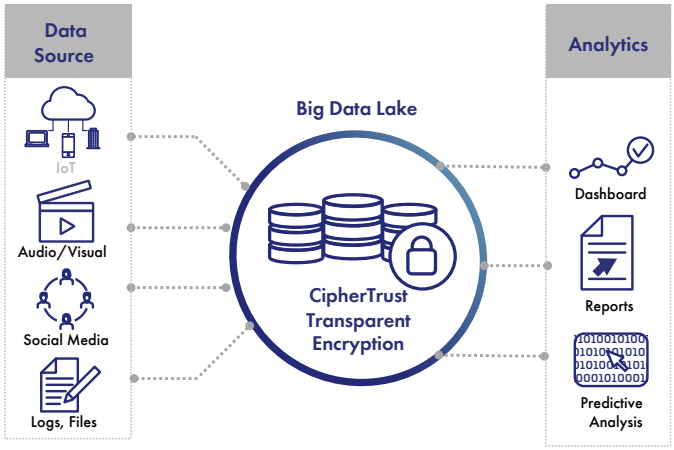

Figure 14: CipherTrust Products Support for Big Data Environments

Solution: CipherTrust Transparent Encryption

CipherTrust Transparent Encryption offers the granular controls, robust encryption, and comprehensive coverage that organizations need to secure sensitive data across their big data environments— including data sources, infrastructure, and analytics. The solution can be used to protect data at the file system level within compute notes (and underlying storage), source data locations, as well as the repositories used for logs and reports. And, this protection extends beyond the system level users/ groups and LDAP/AD users and groups that are enforced by Transparent Encryption agent on a typical server. The solution also enforces policy-based encryption, access controls and data access logging by Hadoop users, groups and zones. This capability provides further protection against privileged users within the big data lake or users within the environment.

A typical deployment includes agents installed on compute nodes, source data servers, and servers accessing log/report repositories. Data is encrypted throughout the environment with appropriate access policies and data access logging controls provided by the CipherTrust Manager. Further, the use of hardware encryption capabilities in underlying compute infrastructure results in minimal overhead from encrypt/decrypt operations. This makes it possible to use the solution even where speed and compute capability are critical. By leveraging the CipherTrust Data Security Platform to secure big data lake environments, organizations can realize the following benefits:

- Compliance: CipherTrust Data Security Platform addresses a broad set of use cases to discover, classify, and protect sensitive data across their big data environments. The platform delivers the comprehensive capabilities that enable organizations to address the demands of evolving regional data protection and privacy laws.
- Prevent privileged-user threats: CipherTrust Transparent Encryption provides the fine-grained, policy-based access controls, including Hadoop granular user access controls, which restrict access to encrypted data. These allow only approved access to data by processes and users as required to meet strict compliance requirements.
- Achieve robust security: Make the most of big data analytics with confidence that the collected and mined data, including that which is sensitive, is protected.

Satisfying Data Privacy and Security Compliance Regulations

The Challenge

As large datasets amounts of sensitive data is migrating to SaaS applications, big data and hybrid-cloud environments business risks are growing because of the following reasons.

- Lack of visibility to where sensitive data resides is leaving gaps in implementing data protection
- Encrypting everything is not an ideal option, since that can impact operational efficiencies
- Compliance gaps are occurring frequently since all sensitive data is not protected everywhere in the enterprise

Solution: CipherTrust Data Security Platform

The CipherTrust Data Security Platform provides an integrated solution for the entire data security journey starting from discovering and classifying sensitive data, analyzing data at risk based on regulatory mandates, and then protecting sensitive data wherever it resides using a variety of CipherTrust Data Protection Connectors.

The CipherTrust Platform enables organizations to meet the following types of compliance requirements that are common across most global compliance regulations and standards, such as GDPR, PCI DSS, HIPAA, NIST and many more.

Compliance Requirement	CipherTrust Platform Product
Identify all assets including sensitive data that needs to be protected	CipherTrust Data Discovery and Classification
Protect sensitive data against unauthorized access and restrict access to sensitive data	CipherTrust Transparent Encryption
Monitor (audit) all authorized/unauthorized user and administrative access to sensitive data	CipherTrust Security Intelligence
Remediate/mitigate risks of sensitive data exposure with strong encryption and data masking (tokenization) technologies	CipherTrust Platform Connectors: • Transparent Encryption • Application Data Protection • Database Protection • Tokenization Intelligent Protection: Automatically mitigates risks by discovering unstructured sensitive data and pro-actively protecting it using Data Discovery and Classification integrated with Transparent Encryption.
Provide a strong encryption key management system that is FIPS certified with elevated root of trust	CipherTrust Manager integrated with Thales Hardware Security Modules

Comprehensive Data Security from Thales

Thales offers a comprehensive portfolio of data protection products that include data discovery and classification, data encryption, tokenization, and centralized key management capabilities, which enable customers to protect business critical data wherever it resides -- in file servers, databases, applications, on-premises, or in multi-cloud environments. The industry leading CipherTrust Data Security Platform from Thales enables you to simplify security, improve operational efficiency, and accelerate time to compliance.

About Thales Trusted Cyber Technologies.

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., is a trusted, U.S. provider of cybersecurity solutions dedicated to U.S. Government. We protect the government's most vital data from the core to the cloud to the edge with a unified approach to data protection. Our solutions reduce the risks associated with the most critical attack vectors and address the government's most stringent encryption, key management, and access control requirements.

For more information, visit www.thalestct.com

Contact us

thalestct.com/contact-us

> thalestct.com <