THALES

CipherTrust Data Security Platform
Discover, Protect and Control

CipherTrust Data Security Platform

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

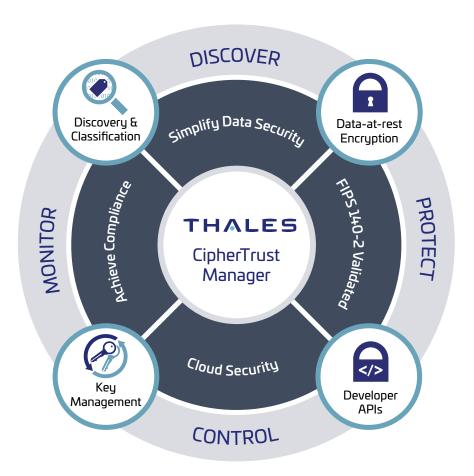**Discover**   **Protect**   **Control**

As data breaches continue at alarming rates, securing sensitive data is critical to all organizations. In addition, organizations struggle to stay compliant with evolving global and regional privacy regulations, and securing the cloud in the face of accelerated adoption brought on by the new demand to support tremendous number of remote employees. IT security organizations seek a data-centric solution that secures the data as it moves from networks to applications and the cloud. When perimeter network controls and endpoint security measures fail, protecting data at rest is the last line of defense.

The CipherTrust Data Security Platform integrates data discovery, classification, data protection and unprecedented 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 less resources dedicated to data security operations, ubiquitous compliance controls, and significantly reduced risk across your business.

Key Features
- Centralized management console
- Monitoring and reporting
- Data discovery and classification
  - Risk analysis with data visualization
- Proactive protection integrated with data discovery and classification
- Data protection techniques
  - Transparent encryption for files, databases and containers
  - 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
  - Unparalleled partner ecosystem of KMIP integrations
  - Multi-cloud key management
  - Database encryption key management (Oracle TDE, big data, MS SQL, SQL Server Always Encrypted, etc.)

Compliance

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

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

Key Benefits

- **Simplify Data Security.** Discover, protect, and control sensitive data anywhere with next-generation unified data protection. The CipherTrust Data Security Platform 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. The centralized and extensible nature of the platform enables new controls to be added using simplified licensing and scripted deployment of connectors to respond to evolving compliance 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, which supports Bring Your Own Key (BYOK) use-cases across multiple cloud infrastructures and SaaS applications.

CipherTrust Data Security Platform Products

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 physical and virtual form-factors that are FIPS 140-2 compliant up to level 3. The CipherTrust Manager can also be rooted to a hardware security module (HSM) such as Thales Luna and Luna Cloud HSM.

CipherTrust Data Discovery and Classification

CipherTrust Data Discovery and Classification locates regulated data, both structured and unstructured, across the cloud, big data, and traditional data stores. A single pane of glass delivers understanding of sensitive data and its risks, enabling better decisions about closing security gaps, compliance violations and prioritizing remediation. The solution provides a streamlined workflow all the way from policy configuration, discovery, and classification, to risk analysis and reporting, helping to eliminate security blind spots and complexities.

CipherTrust Transparent Encryption

CipherTrust Transparent Encryption delivers data-at-rest encryption, privileged user access controls and detailed data access audit logging. Agents protect data in files, volumes and databases on Windows, AIX and Linux OS's across physical and virtual servers in cloud and big data environments. The Live Data Transformation extension is available for 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 risk profiles and pro-actively protect at-risk data using encryption and access controls. It integrates CipherTrust Data Discovery and Classification with CipherTrust Transparent Encryption to improve operational efficiencies, accelerate time to compliance, and pro-actively close security gaps.

CipherTrust Application Data Protection

CipherTrust Application Data Protection 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 and can help reduce the cost and complexity of complying with data security mandates such as PCI-DSS. Tokenization replaces sensitive data with a representative token, so that the sensitize data is kept separate and secure from the database and unauthorized users and systems. The vaultless offering includes policy-based dynamic data masking. Both offerings make it easy to add tokenization to applications.

CipherTrust Database Protection

CipherTrust Database Protection solutions integrate data encryption for sensitive fields in databases with secure, centralized key management and without the need to alter database applications. CipherTrust Database Protection solutions support Oracle, Microsoft SQL Server, IBM DB2 and Teradata databases.

CipherTrust Key Management

CipherTrust Key Management delivers a robust, standards-based 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.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.