cpl.thalesgroup.com

THALES
Building a future we can all trust

Top 10 Reasons to Migrate to the CipherTrust Data Security Platform — For KeySecure Customers

You relied on the KeySecure platform over many years to provide centralized key management and data protection throughout your enterprise — on premises and in AWS. To stay a step ahead of dynamic cybersecurity threats and protect your investments, Thales delivered the next generation of data security — the CipherTrust Data Security Platform (CDSP).

CDSP combines the strengths of two industry-leading data protection companies, Gemalto and Vormetric, supports a comprehensive set of use cases that you already rely on, manages cloud-native keys painlessly, and offers several new capabilities to keep pace with the latest innovations.

CDSP increases efficiency by enabling you to do more with fewer resources. You can manage your keys with a single pane of glass and rely on a centralized audit trail to meet data protection compliance mandates that are becoming more stringent. Next generation data protection increases efficiency and spans more environments, systems, applications, processes and users. The CipherTrust Data Security Platform is centered around a key and policy manager, CipherTrust Manager (CM), that centralizes access to the portfolio of data protection Connectors and an ecosystem of partner integrations.

As the central management point for CDSP, CM simplifies key lifecycle management tasks for all of your encryption keys across cloud, virtual and physical environments. CM manages secure key generation, backup/restore, clustering, deactivation, and deletion, and provides access to Connectors and partner integrations that support a variety of use cases including data discovery, data-at-rest encryption, enterprise key management, and cloud key management.

This brief captures the major reasons for current KeySecure customers to migrate to the new CipherTrust Data Security Platform now.

1. **New Simplified Management Console with Self-service Licensing**

   The CipherTrust Manager (CM) console provides a self-service licensing portal that gives customers better visibility and control of which Connector licenses are in use.

   CM centralizes management of policies and keys for all CipherTrust Connectors and partner integrations.

2. **Improved Monitoring and Alerting**

   With CipherTrust Manager's improved compliance monitoring, organizations can forward syslog alerts to integrate seamlessly with Elastic Search, Loki and security information and event management (SIEM) systems. CipherTrust Manager (CM) includes tracking of all administrator access and encryption key state and policy changes in multiple log formats (RFC-5424, CEF, LEEF). Additionally, CM offers support for Splunk log analysis and Prometheus monitoring tools. Customers can generate pre-configured and customizable email alerts (SNMP v1, v2c, v3).

3. **New Data Discovery and Classification**

   Organizations can rapidly understand business risks and automate remediation actions due to visibility into where their sensitive data resides across on prem and all major cloud environments.

4. **Application-level Encryption**

   To simplify integration to the platform, CipherTrust Application Data Protection (CADP) offers developer kits in various programming languages (Java, C/C++, .NET/.NET CORE). Alternatively, applications can automate key management and encryption operations by leveraging field-proven Crypto APIs (NAE) to interact remotely with CipherTrust Manager.

   Integrated CipherTrust Tokenization offers application-level tokenization services in two flexible solutions. Vaultless Tokenization with Dynamic Data Masking and Vaulted Tokenization. Both tokenization solutions secure and anonymize sensitive assets — whether the assets reside in the data center, big data environments or the cloud.

5. **Transparent Encryption for File Systems and Databases**

   CipherTrust Transparent Encryption (CTE) delivers data-at-rest encryption with privileged user access control for files, volumes and databases, without requiring any code change to applications. CTE offers support for Amazon S3, Live Data Transformation, SAP HANA, Teradata and file encryption in user space on Linux FUSE.

6. **DevSecOps-friendly**

   DevSecOps teams can now transparently protect sensitive data in cloud applications and file stores without modifying legacy or cloud-native applications. See CipherTrust Data Protection Gateway (DPG) and CipherTrust Transparent Encryption for Kubernetes (CTE-K8s).

   To simplify deployment of applications integrated with key management capabilities and automate development and testing of administrative functions, CipherTrust Manager (CM) offers REST interfaces, in addition to KMIP and NAE-XML APIs. CM also has its own REST API Playground that allows customers to experiment with administration, key management, user management, and crypto operations.

7. **Multi-cloud Key Management**

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

   - Multiple clouds — AWS, Azure, Google Cloud, Oracle, Salesforce and SAP
   - Native cloud key management — amplifies the benefits of native keys with outstanding UI that includes a single pane of glass view across multiple accounts, regions, subscriptions and projects
   - Increased customer control — Bring Your Own Key (BYOK) and Hold Your Own Key (HYOK) are supported across multiple cloud infrastructures and SaaS applications

8. **Unparalleled Partner Ecosystem**

   Through standard APIs, the CipherTrust Data Security Platform offers an extensive set of partner integrations with leading enterprise storage, server, database and SaaS vendors including Netapp, DellEMC, VMware, Microsoft, IBM, Oracle TDE, Teradata, ServiceNow, AWS, Azure, and Google Cloud.

9. **Hybrid High-availability Clustering**

   To ensure optimum processing in high-availability environments, regardless of whether the workload location is an on-prem data center, in the cloud, or a combination of the two, CipherTrust Manager offers a choice of clustering physical and virtual appliances.

10. **FIPS 140-2 Certified HSMs**

    CipherTrust Manager (CM) provides a stronger security posture using a FIPS 140-2 Level 3 boundary to enhance key management use cases.

    For better key entropy, CM provides several options to integrate with a FIPS 140-2 validated physical or virtual HSM as a secure root of trust.

    - Built-in HSM crypto accelerator card on a CM k570 appliance.
    - Network-attached Luna HSM with HA clustering
    - Cloud HSM (Data Protection on Demand service) for several major cloud service providers