10 Reasons to Choose
CipherTrust Data Security Platform

THALES
Building a future we can all trust

CipherTrust Data Security Platform

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

Discover   Protect   Control

From tackling advanced new cyberthreats to ensuring data sovereignty and compliance, organizations are under pressure to manage an increasingly complex and disparate security landscape. Unifying data discovery, protection and control on a single, next-generation platform, CipherTrust Data Security Platform gives you complete control.

1. Comprehensive Data Protection

CipherTrust Data Security Platform supports a broad set of data protection use-cases. It's a single control point for the entire data security lifecycle and include centralized key management, data encryption, live data transformation, tokenization and dynamic data masking, role-based access and security intelligence.

2. Integrated Data Discovery and Classification

Data discovery and classification delivers complete visibility to protect your sensitive data wherever it resides – across on-premises, big data and cloud environments. Understand your business risks and automate remediation using a variety of CipherTrust data protection connectors.

3. Support for Broadest Deployment Environments

Protect structured and unstructured data-at-rest across your organization – in files, volumes, databases and applications on Windows, AIX and Linux OS's, across physical/virtual servers and in containers, cloud and big data environments.

4. Simple, Centralized Management

Manage your entire data security and streamline connector administration with self-service licensing – all from one UI on a single console. Set up policies and integrate syslog/SNMP alerts with your existing workflows and security information and event management (SIEM) systems with ease.

5. FIPS 140-2 Validated HSMs and Connectors

Designed to meet the strictest compliance requirements, many of the data protection connectors are FIPS validated. The CipherTust Manager physical appliance is equipped with an embedded FIPS 140-2 Level 3 HSM for a secure internal root of trust. Other options include virtual and physical appliances to use an external HSM as a root of trust. For example, supported HSMs are Luna Network HSM, Luna Cloud HSM on Data Protection on Demand and AWS CloudHSM.

6. Multi-Cloud Key Management

CipherTrust Cloud Key Management (CCKM) increases efficiency by reducing the operational burden—even when all of the cloud keys are native keys. Giving customers lifecycle control, centralized management within and among clouds, and visibility of cloud encryption keys reduces key management complexity and operational costs. 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. Does not require customer to set up separate CCKM instances.

- Increased customer control – Bring Your Own Key (BYOK) and Hold Your Own Key (HYOK) are supported across multiple cloud infrastructures and SaaS applications.

- Metadata is collected and laid out in the same order for every cloud provider, removing the need to look for data in disparate places.

7. 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 and CipherTrust Transparent Encryption for Kubernetes. 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.

8. Flexible Deployment Choices

Deploy as a physical or virtual appliance with hybrid clustering for high-availability environments to ensure optimum processing regardless of the workload location (data center or cloud). CipherTrust Manager also provides multi-tenancy and separation of duty capabilities required to support large enterprise environments.

9. Accelerate Time to Compliance

From data discovery and classification to encryption, access control, audit logs, tokenization, and key management, CipherTrust delivers the capabilities to assure compliance – with Payment Card Industry Data Security Standard (PCI DSS), General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and other global/regional data protection and privacy laws.

10. 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.

Complete Control, Seamless Protection

Whether you're building your encryption strategy, meeting compliance mandates or moving to the cloud, CipherTrust brings everything together in a single, powerful, next-generation platform.

About Thales

Today's businesses and governments depend on the cloud, data and software to deliver trusted digital services. That is why the most recognized brands and organizations around the world, rely on Thales to help them protect sensitive information and software wherever it is created, stored or accessed – from the cloud and data centers to devices and across networks. As the global leader in data security, identity & access management, and software licensing, our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, create more value from their software and deliver seamless digital experiences for millions of consumers every day.

cpl.thalesgroup.com