thalestct.com

THALES

Top 10 Reasons for Protecting Your Organization with CipherTrust Data Security Platform

The CipherTrust Data Security Platform unifies data discovery, classification, data protection and provides unprecedented granular access controls with centralized key management – all on a single platform to meet data privacy and security regulations. This solution removes complexity from deploying data security, 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. This brief captures the major reasons for adopting the new CipherTrust Data Security Platform now.

1. Comprehensive Data Protection

CipherTrust Data Security Platform supports a broad set of data protection use-cases that deliver centralized key management, data encryption, live data transformation, tokenization with dynamic data masking, privileged user access controls and security intelligence across the entire data security lifecycle.

2. Integrated Data Discovery and Classification

The platform offers data discovery and classification functionality for your organization to get a clear visibility into where your sensitive data resides across on-premises, big data and cloud environments. It enables you to understand your business risks and automate remediation using a variety of CipherTrust Data Protection Connectors.

3. Support for Broadest Deployment Environments

CipherTrust Data Security Platform offers a variety of data protection solutions that protect structured and unstructured data-at-rest wherever it resides, such as in files, volumes, databases and applications on Windows, AIX and Linux OS's across physical/virtual servers, in containers, cloud and big data environments.

4. Simplified Management Console

The platform provides a management console that streamlines connector administration with self-service licensing. From a single pane of glass, your organization can setup policies and syslog/ SNMP alerts that can be integrated with your existing workflows, and security information and event management (SIEM) systems.

5. FIPS 140-2 Validated HSMs and Connectors

CipherTrust Data Security Platform is designed to meet the strictest compliance requirements. Many of the data protection connectors are FIPS validated. In addition, the CipherTust Manager physical appliance is already 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. Supported HSMs are Luna Network HSM, Luna Cloud HSM on Data Protection onDemand, AWS CloudHSM, and Thales TCT's T-Series HSMs.

6. Adaptable Multi-Cloud Security

The platform offers several options to securely move workloads to the cloud and hosted environments, and repatriate data back on-prem, knowing that your data remains in your control

- Virtual CipherTrust Manager for all major public clouds and private hypervisors.
- Advanced multi-cloud Bring Your Own Encryption (BYOE) solutions to secure your data and reach compliance rapidly and effectively.
- CipherTrust Cloud Key Manager simplifies Bring Your Own Key(BYOK) use-cases across multiple cloud infrastructures and SaaS applications with automation and key life-cycle management.

7. Developer-Friendly APIs

The platform includes a range of products that enable developers to add strong security for data at the application layer to protect against threats without becoming crypto experts. Choices include tokenization, key management and encryption services accessible with REST, KMIP, or with Java, C and .Net bindings to PKCS#11 standard libraries. This solution also assures seperation of duties, because your IT team remains in control of encryption keys, tokenization rules and access policies.

8. Flexible Deployment Choices

CipherTrust Manager can be deployed either 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 that are required to support large enterprise environments.

9. Accelerate Time to Compliance

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 like the 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. Unmatched Partner Ecosystem

The platform offers an extensive set of partner integrations with leading enterprise storage, server, database and SaaS vendors such as, NetApp, Dell EMC, Pure Storage, Microsoft, IBM, Oracle TDE, Teradata, ServiceNow, AWS, Azure, Google Cloud and many more.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled. For more information, visit thalestct.com

3465 Box Hill Corporate Center Drive, Suite D, Abingdon, MD 21009 • 443-484-7070 • info@thalestct.com
thalestct.com