Product Brief

CipherTrust Transparent Encryption

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

Ensure the protection of sensitive data with advanced data-at-rest encryption, robust access controls, and comprehensive audit logging for data access. Achieve compliance and adhere to best practices with a reliable hardware-accelerated encryption solution that secures files, volumes, and connected cloud storage across physical, virtual, and cloud environments.

Challenge: Securing Sensitive Data Across Changing Environments and Increasing Threats

Safeguarding sensitive data requires much more than just securing a data center's on-premises databases and files. The typical enterprise today uses three or more IaaS or PaaS providers, along with fifty or more SaaS applications, big data environments, container technologies, and their own internal virtual environments and private clouds.

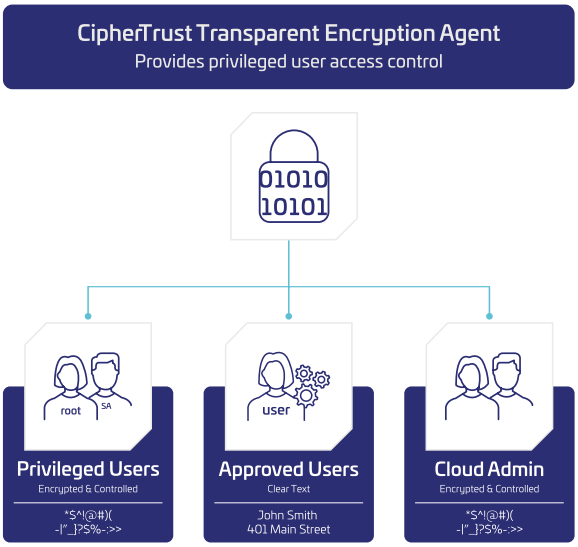
To further complicate the problem, cyberattacks have grown in sophistication and power. New compliance and regulatory mandates around protection of sensitive information keep on coming, and existing regulations have become more stringent. SAS PCE Enterprise IAM can seamlessly integrate with existing infrastructure and applications, minimizing disruptions and ensuring smooth operations.

Solution: 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 that helps organizations meet compliance and best practice requirements for protecting data, wherever it resides. The FIPS 140-3 L1 certified CipherTrust Transparent Encryption agent resides at the operating file-system or device layer, and encryption and decryption is transparent to all applications that run above it. CipherTrust Transparent Encryption provides rich access controls, which allow organizations to determine who can access data, when they can access it, and what type of access they have.

Key Requirements for Securing Sensitive Data-at-Rest:

- **Compliance and best practices:** Meet encryption, access control, and data access logging requirements with a proven, hardware-accelerated encryption solution. Secure files, volumes, and linked cloud storage, while enabling detailed access controls and audit logging across physical, virtual, and cloud environments.
- **Simple, scalable deployment:** Easily deploy a solution that scales across multiple clouds, on-premises, big data, and container environments. Centralized key management, encryption, and access policies ensure streamlined operations.
- **Privileged user access control:** Protect sensitive data by enabling administrators to continue their work while preventing unauthorized access by potential threats among users and groups.



- **Actionable security insights:** Utilize detailed, actionable security event logs to gain valuable insights into file access activities and quickly detect and stop potential threats.
- **Broad platform support:** Secure both structured and unstructured data across Linux, FreeBSD, AIX, and Windows systems. Extend transparent encryption and access controls to data stored in S3 buckets.
- **No downtime for encryption and re-keying:** Use the Live Data Transformation connector to eliminate downtime during initial encryption and re-keying processes. This unique feature sets CipherTrust Transparent Encryption apart from other solutions.

Key Features

Transparent data protection: Continuously enforces file-level encryption that protects against unauthorized access by users and processes and creates detailed data access audit logs of all activities without requiring changes to applications, infrastructure, systems management tasks, or business practices.

Seamless and easy to deploy: CipherTrust Transparent Encryption agents are deployed on servers at the file system or volume-level and support both local disks as well as cloud storage environments, such as Amazon S3 and Azure Files.

Define granular access controls: Apply granular, least-privileged user access policies that protect data from external attacks and

misuse by privileged users. Specific policies can be applied by users and groups from systems, LDAP/Active Directory, Hadoop and containers. Controls also include access by process, file type, time of day, and other parameters.

High-performance hardware accelerated encryption: CipherTrust Transparent Encryption only employs strong, standard-based encryption protocols, such as the Advanced Encryption Standard (AES) for data encryption and Elliptic Curve Cryptography (ECC) for key exchange. Encryption overhead is minimized using the AES hardware encryption capabilities available in modern CPUs.

Comprehensive security intelligence: Identify and stop threats faster with detailed data access audit logs that not only satisfy compliance requirements, but also enable data security analytics.

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

Broadest system and environment support: The agent is available for a broad selection of Windows, Linux, and AIX platforms, and can be used in physical, virtual, cloud, Kubernetes and big data environments, regardless of the underlying storage technology.

Advanced Security Benefits

Integration with cloud and container environments: Protects data in dynamic cloud and container environments.

Key rotation: Automatically rotates encryption keys to enhance security.

Data destruction: Ensures sensitive data is permanently erased when no longer needed.

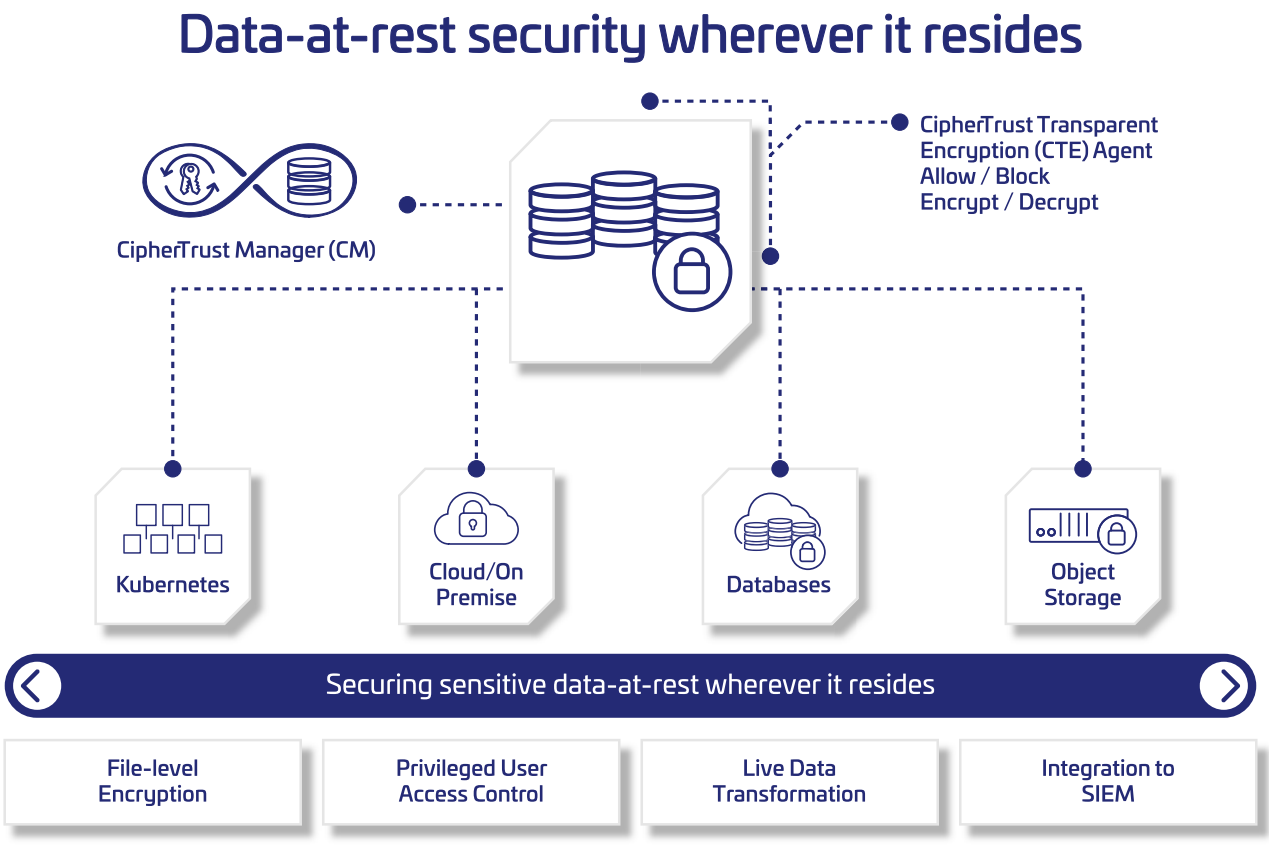
Zero-downtime data transformation: Live Data Transformation option eliminates the downtime required for initial encryption and scheduled rekeying operations. This patented technology allows for databases or files to be encrypted or re-keyed with a new encryption key while the data is in use without taking applications off-line.

SAP HANA and teradata qualified: SAP and Teradata have qualified CipherTrust Transparent Encryption with SAP HANA and Teradata database respectively to deliver data encryption, key management, privileged user access control, and granular file access audit logs

CipherTrust transparent encryption userspace: Provides scalable and robust file encryption solution based on Linux FUSE that is not affected by kernel upgrades on Linux servers.

Solution Architecture

Deployment consists of CipherTrust Transparent Encryption connectors and CipherTrust Manager appliances. Policy and key management is centralized at the CipherTrust Manager. The CipherTrust Manager is available as a FIPS 140-2 Level 1 or FIPS 140-2 Level 3 with HSM compliant appliance.



Benefits of CipherTrust Transparent Encryption:

Enhanced Data Security:

Data-at-rest encryption: Protects sensitive data from unauthorized access, even if the underlying storage is compromised.

Centralized key management: Manages encryption keys securely, reducing the risk of key exposure.

Privileged user access control: Controls access to encrypted data, even for privileged users, ensuring data confidentiality.

Improved Compliance:

Detailed data access audit logging: Provides a comprehensive audit trail, helping organizations meet compliance requirements such as PCI DSS, HIPAA/HITECH, and GDPR.

Strong data protection: Enhances overall data security posture, reducing the risk of data breaches and regulatory fines.

Operational Efficiency:

Transparent encryption: Encrypts data without requiring changes to applications or user workflows, minimizing disruption to business operations.

Scalability: Easily scales to protect large volumes of data across diverse environments, simplifying management.

Flexible deployment: Supports various deployment options to adapt to different use cases.

Additional Benefits:

Integration with cloud and container environments: Protects data in dynamic cloud and container environments.

Key rotation: Automatically rotates encryption keys to enhance security.

Data destruction: Ensures sensitive data is permanently erased when no longer needed.

By leveraging these benefits, CipherTrust Transparent Encryption empowers organizations to safeguard their sensitive data, meet compliance obligations, and maintain operational efficiency.

CipherTrust Data Security Platform

CipherTrust Transparent Encryption is part of the CipherTrust Data Security Platform. Featured in Gartner's Market Guide to Data Security Platforms, CipherTrust Data Security Platform is an integrated set of data-centric solutions that remove complexity from data security, accelerate time to compliance, and secure cloud migrations.

The CipherTrust Platform unifies data discovery, classification, data protection, and centralized management for keys and secrets into a single platform. This results in fewer resources dedicated to security operations, ubiquitous compliance controls, and significantly reduced risk across your business.

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 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

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us