cpl.thalesgroup.com

THALES
Building a future we can all trust

CipherTrust Transparent Encryption
UserSpace

Challenge: securing sensitive data across changing environments and increasing threats

Safeguarding sensitive data in on-premises data centers, big data and in public or private cloud (IaaS/PaaS) environments transparent to applications can be hard to manage, especially in Linux environments, due to the multiple flavors of Linux and the frequency of OS updates.

To further complicate the problem, cyber-attacks have grown in sophistication and power. New compliance and regulatory mandates around protection of sensitive information keep coming, and existing regulations have become more stringent

Solution: CipherTrust Transparent Encryption UserSpace

CipherTrust Transparent Encryption UserSpace is a part of the CipherTrust Transparent Encryption suite of products, which provides a robust and scalable file system level encryption and access control solution for Linux servers in the distributed enterprise.

CipherTrust Transparent Encryption UserSpace works across multiple flavors of Linux OS that makes deploying the solution easy for customers. Traditionally, these efforts required multiple agents to be tested per Linux OS version. CipherTrust Transparent Encryption UserSpace, eliminates these hurdles using a single installation package across all Linux OS and OS kernel upgrades without cross-checking compatibility. It provides encryption and access control with centralized key management without changes to infrastructure or applications.

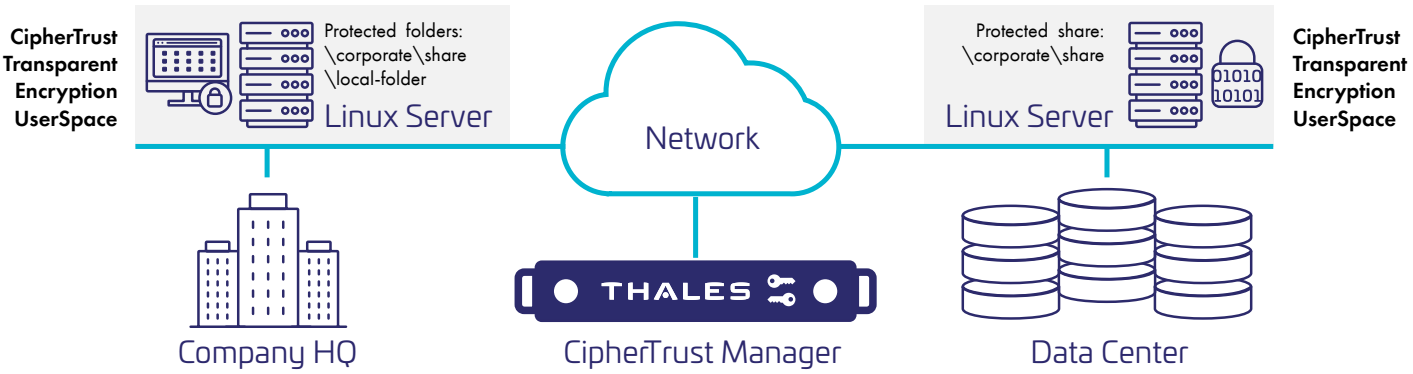
Once deployed, files containing sensitive data are rendered useless in the event of a breach, misuse or hijacking of privileged accounts, physical theft of servers, and other potential threats.

CipherTrust Transparent Encryption UserSpace works in conjunction with a FIPS 140-2 up to Level 3 compliant CipherTrust Manager, which centralizes encryption key and policy management for the CipherTrust Data Security Platform. The solution encrypts sensitive data, such as credit card numbers, personal information, logs, passwords, and more in a broad range of files, including word processing documents, images, database files, archives, and backups.

Once deployed and initiated on a server, CipherTrust Transparent Encryption UserSpace encrypts and decrypts data in local and mapped network folders at the file system level based on policies – without disruption to business operations, application performance, or end-user experience.

Secure sensitive data-at-rest wherever it resides

- Meet compliance and best practice requirements for encryption, access control, and data access logging using a proven hardware accelerated encryption solution, that secures files, while enabling access control and data access audit logging.
- Deployment is simple, scalable and fast with centralized key management, encryption, and access policies that reach across multiple clouds, on-premises, and within databases, file shares and big data environments.
- Easily implement privileged user access controls to enable administrators to work as usual but protect against users and groups that are potential threats to data.



Key advantages

Transparent data protection. CipherTrust Transparent Encryption UserSpace 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 UserSpace agents are deployed on Linux servers at the file system level and are agnostic to Linux kernel patches. Supports continuous Linux server patching without agent changes.

Lower maintenance costs. It is based on Linux FUSE libraries which allows it to be deployed across different Linux distributions. Not requiring continuous updates allows user to keep administration costs low.

Granular access controls. Specific policies can be applied to protect data from external attacks and misuse by privileged users. Controls also include access by process, file type, and other parameters.

High-performance hardware accelerated encryption. It only employs strong, standard-based encryption protocols, such as the Advanced Encryption Standard (AES) for data encryption. Encryption overhead is minimized using the AES hardware encryption capabilities available in modern CPUs.

Achieve Compliance. CipherTrust Transparent Encryption UserSpace helps achieve compliance with a variety of regulations that require encryption of data including credit card numbers for PCI-DSS compliance, electronic patient health information (EPHI) for HIPAA, and personal identifiable information (PII) to comply with many regional data privacy regulations.

Highlights

Transparent, Strong, and Efficient Encryption

- Apply transparent and automated file system-level encryption in physical, virtual, and cloud environments
- Define and enforce granular access control policies

Privileged User Control

- Prevent rogue root administrators from impersonating other users and accessing protected data

Secure Data Archiving and Destruction

- Keep data encrypted and unreadable to server administrators performing back-up and restore tasks
- Ensure all secured, sensitive data is rendered unreadable in the event data destruction is required

Easy Implementation and Management

- Utilize remote, silent automation tools for quick and easy deployment in large and small environments
- Streamline administration with centralized policy and key management in FIPS compliant hardware
- Built-in key rotation capability

Achieve Compliance

- Ensure separation of duties
- Track and audit user access to protected data and keys

Multi-language Support

- Encrypt files and folders written in Arabic, Japanese, Korean and other languages. Encryption and collaboration aren't mutually exclusive across geographies.

CipherTrust Data Security Platform

CipherTrust Transparent Encryption UserSpace is part of the CipherTrust Data Security Platform. The CipherTrust platform unifies data discovery, classification, data protection, and provides unprecedented granular access controls, all with centralized key management. This simplifies data security operations, accelerates time to compliance, secures cloud migrations, and reduces risk across your business.

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.

> cpl.thalesgroup.com <

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