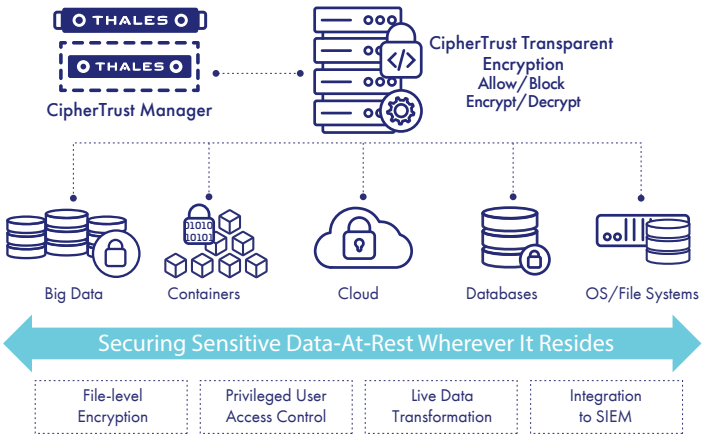
cpl.thalesgroup.com

THALES

Top 10 reasons CipherTrust Transparent Encryption protects your data, wherever it resides

The volume of data that your organization is using and storing has likely grown significantly in the past year alone. Compliance with the numerous regional and global privacy laws and regulations is getting more complex and challenging. Every day brings reports of new data breaches which damage reputations as well as bottom lines. There are multiple options available for securing data. Finding a seamless approach that avoids modification of your applications to protect sensitive assets is critical, especially in cases where rapid deployment is important. Sensitive data discovery and automated protection in a streamlined workflow is highly desirable.

CipherTrust Transparent Encryption delivers data-at-rest encryption with centralized key management, privileged user access control and detailed data access audit logging. This protects data wherever it resides - on-premises, across multiple clouds and within big data and container environments. The deployment is simple, scalable and fast, with agents installed at operating file system or device layer - encryption and decryption is transparent to all applications that run above it. With CipherTrust Transparent Encryption you satisfy data security compliance and best practice requirements with minimal disruption, effort and cost. It can be configured to work seamlessly



with our data discovery and classification solution to enable integrated discovery and protection in a single step, delivering rapid compliance and reduced risk. To help you better understand the advantages of our offering, we have compiled a top 10 reasons for using CipherTrust Transparent Encryption.

Transparent operation

1 Operates seamlessly in the background

Any data protection system needs to be easy to deploy and use, otherwise it will be an unwanted (and potentially costly) distraction for your organization.

There are no application changes necessary to deploy and encrypt data in files and folders with CipherTrust Transparent Encryption. It delivers fast, transparent file-level encryption for your data-at-rest. Operating rapidly and seamlessly, the encryption or decryption process is transparent to all your applications running above it. Importantly, it does not derail any of your business processes, user tasks or administration workflows.

2 Secures data everywhere

Your data will likely be in many formats and in various locations – securing only a section of your overall data footprint may not keep you safe from a data breach.

With CipherTrust Transparent Encryption you can encrypt your data, wherever it resides. It offers the ability to address a comprehensive range of structured and unstructured data types with support for on-premises, cloud, big data and container environments – nothing important is outside the scope of its protection capabilities.

Enhanced security

3 Mitigates ransomware attacks

Ransomware is a vicious type of malware that cybercriminals use to block organizations like yours from accessing business critical files, databases, or entire computer systems, until you, the victim, pay a ransom. It is a form of cyber extortion.

Access policies can be defined to create a whitelist of "trusted" applications to prevent any untrusted binaries (e.g. ransomware) from accessing data stores protected by CipherTrust Transparent Encryption and to prevent privileged users from accessing user data in files and databases. These access policies enable you to block any rogue binaries from encrypting files/databases/devices, even if the intruder has execute permissions for that binary and read/write permissions to the target file that contains business critical data. CipherTrust Transparent Encryption can stop privilege escalation attacks, by preventing administrators from reading/writing to protected folders/files/devices.

4 Protects against unauthorized data access

Encrypting your data is not the end of the story – you need to be able to provide access to authorized individuals to access and read the data in question.

This is where the role-based access policies at the core of CipherTrust Transparent Encryption come into play. They enable you to control who, what, where, when and how your data can be accessed. Access controls are available for system level users and groups as well as LDAP, Active Directory, Hadoop and Container users and groups. It is easy to implement privileged user access controls to enable administrators to work as usual, but protect against users and groups that are potential threats to your data.

Easy deployment

5 Avoids system downtime

No one wants to take their systems offline for hours or days to secure their data.

CipherTrust Transparent Encryption utilizes agents for its cryptographic operations. The agents are installed at the operating file system or device layer – this is a highly scalable and transparent process, taking place in the background without impacting any of your systems or applications, including their performance. Nothing needs to be taken offline during the installation process. When you are ready to start the encryption of your selected data, our zero downtime data transformation capability is invaluable. Using the Live Data Transformation option means that system downtime is eliminated completely for the initial encryption operations, enabling your data to be secured, no matter its size, while your teams keep working as normal.

6 Covers all major platforms and operating systems

Ensuring that you are able to secure data across all the different platforms your organization is using is an important consideration when selecting an encryption solution.

CipherTrust Transparent Encryption offers tight integration and optimization for each particular operating system kernel. It delivers enhanced performance, leveraging hardware-accelerated encryption, by making use of the built-in encryption capabilities of some of the latest CPUs from AMD, Intel and IBM. Bring Your Own Encryption (BYOE) is easy to adopt in conjunction with the solution. It has support for all major platforms and operating systems together with some of the latest cloud approaches including Amazon S3 buckets and Azure Disk and File Storage. A range of extensions to the CipherTrust Transparent Encryption connector (including Live Data Transformation, SAP HANA, Efficient Storage and Teradata Protection) provides optimized encryption support for specific platforms and configurations that you may already be using or considering.

7 Incorporates both internal and external keys

Sometimes you need to use cryptographic keys that already exist from other systems or which are provided by a third party. If your chosen data encryption solution is inflexible, you may experience significant issues.

We designed CipherTrust Transparent Encryption to be as flexible as possible – importantly we do not insist that all keys are created by the CipherTrust platform. You have the ability to leverage keys that you (or a trusted third party) generated outside of the CipherTrust Data Security Platform. The ability to import such keys is an alternative to using keys generated by the platform. The end result is identical – you receive fast, transparent and secure protection of your data.

Rapid compliance

8 Facilitates integrated discovery and protection

Failing to protect sensitive data rapidly after discovery could leave you vulnerable and not compliant with data privacy laws and regulations. A mix and match of data discovery and protection tools from different vendors adds complexity and often leads to much higher operating costs.

The CipherTrust platform offers intelligent protection, which is a tight integration between CipherTrust Data Discovery and Classification and CipherTrust Transparent Encryption – enabling you to discover and then protect data automatically in a single step with no manual intervention. This platform feature which utilizes CipherTrust Manager to configure and manage both the discovery and protection connectors is known as CipherTrust Intelligent Protection - a proven solution to protect your data and reduce your risk.

9 Simplifies compliance reporting

Proving your handling of data complies with the various laws and regulations can be an onerous task, especially if you are still adopting a manual, ad-hoc approach.

As you might expect, CipherTrust Transparent Encryption has a range of capabilities which make your life easier when needing to prove your data is in compliance. It supports the creation of reports required by auditors as part of compliance regulations – you can export log files generated by the encryption solution to a System Information and Event Management (SIEM) solution of your choosing – we support standard formats for logging including syslog, Common Event Format (CEF) and Log Event Extended Format (LEEF). All access and encryption attempts (successful or failed) are logged, enabling you to present the complete picture to both the internal and external auditors as required.

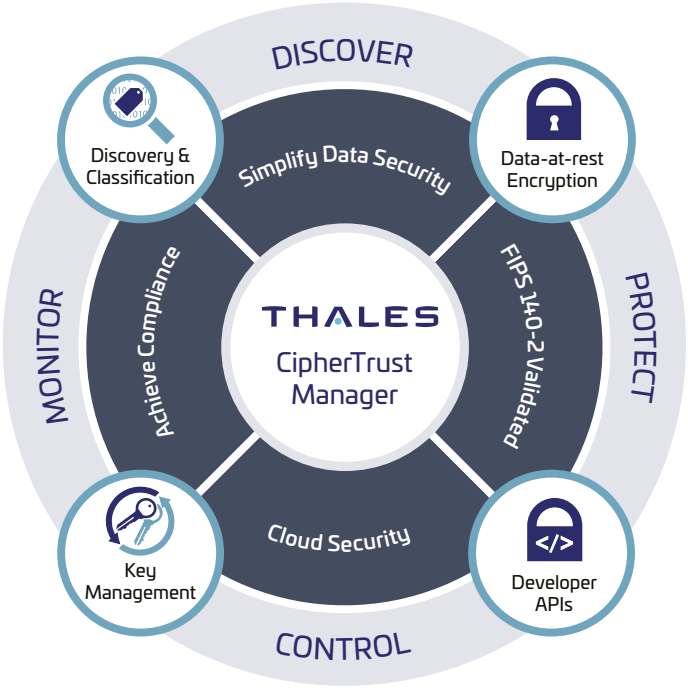
10 Underpins business continuity

Any encryption solution that interferes in a detrimental manner with the day-to-day operations of a business is unlikely to experience significant adoption.

You can be assured that the deployment of CipherTrust Transparent Encryption will enable your business to function, uninterrupted. For example, the solution can be configured to encrypt files while leaving the metadata in the clear. It supports business continuity for administrators and system-level users without violating privacy and security requirements – a wide range of access control policy settings enables a granular approach to be implemented to facilitate the specific needs of all your data users. The integrity, security and availability of your data is assured by using our solution.

CipherTrust Data Security Platform

CipherTrust Transparent Encryption is part of the CipherTrust Data Security Platform. The CipherTrust platform unifies data discovery, classification, and data protection. It provides unprecedented granular access controls and 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.

THALES

Contact us

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

> cpl.thalesgroup.com <