cpl.thalesgroup.com

THALES

CipherTrust Transparent Encryption

Advanced data-at-rest encryption, access control and data access audit logging

White Paper

Contents

Introduction

Enterprise digital transformation and increasingly sophisticated IT security threats have resulted in a progressively more dangerous environment for enterprises with sensitive data, even as compliance and regulatory requirements for sensitive data protection rise. With attacks adapting on a daily or even hourly basis, even next-generation network and endpoint defenses consistently fail to stop enterprise network penetration. At the same time, digital transformation is expanding the attack surface available to adversaries beyond traditional enterprise boundaries, as organizations embrace the business advantages available from these new solutions.

Just as no single attack method is responsible for all increased threats to enterprise data, no single digital transformation technology is responsible for all increased risks from these new environments – as each technology adopted presents unique data security challenges. However, the number and complexity of these new technologies and the individualized approach required to secure data throughout each environment combine to compound the problem.

Within this environment of increased risks to sensitive data, enterprises require the ability to limit access to sensitive information to only those users, groups, and processes that require the use of the data – and no more. This need extends across traditional data centers, cloud environments, SaaS implementations, and to the data stores of every digitally transformative environment. What is required is a way to make sensitive data useless (and valueless) when not in use and then to control access to the levers that make the data useful again, when it is needed by a legitimate user. This is what transparent encryption with user access control does.

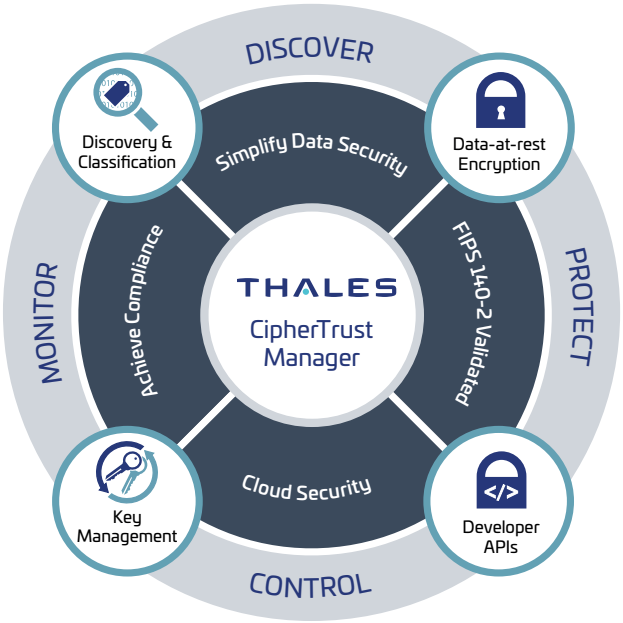
CipherTrust Transparent Encryption enables quick, effective and transparent protection of data at the system level without derailing business processes, user tasks, and administrative workflows. With a single set of data security controls, information stored within physical and virtual systems, big data environments, containers, and linked cloud storage are protected at the file system or volume level across data centers and cloud environments. The result is greatly reduced risk, and an enhanced capability to meet compliance and regulatory data security requirements.

The CipherTrust Data Security Platform from Thales

The CipherTrust Data Security Platform is composed of an integrated suite of products built on a common, extensible infrastructure with efficient, centralized key and policy management. As a result, your security teams can address your data security policies, compliance mandates, and best practices, while reducing administration effort and total cost of ownership. The platform offers capabilities for protecting and controlling access to databases, files and containers—and can secure assets residing in cloud, virtual, big data and physical environments. This scalable, efficient data security platform enables you to address your urgent requirements, and it prepares your organization to nimbly respond when the next security challenge or compliance requirement arises.

Simplify Data Security

Discover, protect, and control sensitive data anywhere with next-generation unified data protection. The CipherTrust Data Security Platform simplifies data security administration with 'single pane of glass' centralized management console that equips organizations with powerful tools to discover and classify sensitive data, combat external threats, guard against insider abuse, and establish persistent controls, even when data is stored in the cloud or in any external provider's infrastructure. Organizations can easily uncover and close privacy gaps, prioritize protection, and make informed decisions about privacy and security mandates before a digital transformation implementation.



Accelerate Time to Compliance

Regulators and auditors require organizations to have control of regulated and sensitive data and reports to prove it. 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. These controls can be quickly added to new deployments or in response to evolving compliance requirements. The centralized and extensible nature of the platform enables new controls to be added quickly through the addition of licenses and scripted deployment of the needed connectors in response to new data protection requirements.

Secure Cloud Migrations

The CipherTrust Data Security Platform offers advanced encryption and centralized key management solutions that enable organizations to safely store sensitive data in the cloud. The platform offers advanced multi-cloud Bring Your Own Encryption (BYOE) solutions to avoid cloud vendor encryption lock-in and ensure the data mobility to efficiently secure data across multiple cloud vendors with centralized, independent encryption key management. Organizations that cannot bring their own encryption can still follow industry best practices by managing keys externally using the CipherTrust Cloud Key Manager. The CipherTrust Cloud Key Manager supports Bring Your Own Key (BYOK) use-cases across multiple cloud infrastructures and SaaS applications. With the CipherTrust Data Security Platform, the strongest safeguards protect an enterprise's sensitive data and applications in the cloud, helping the organization meet compliance requirements and gain greater control over data, wherever it is created, used, or stored.

The CipherTrust Transparent Encryption Solution

Introduction

CipherTrust Transparent Encryption software for enterprises 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, and encryption and decryption is transparent to all applications that run above it. CipherTrust Transparent Encryption is designed to meet data security compliance and best practice requirements with minimal disruption, effort, and cost. Implementation of the encryption software is seamless keeping both business and operational processes working without changes even during deployment and roll out.

Meet compliance requirements for encryption and access control

Encryption, access controls, and data access logging are basic requirements or recommended best practices for almost all compliance and data privacy standards and mandates, including PCI DSS, HIPAA/Hitech, GDPR and many others. CipherTrust Transparent Encryption delivers the controls required without operational or business process changes.

Scalable encryption

The CipherTrust Transparent Encryption agent runs at the file system or volume level on a server. The agent is available for a broad selection of Windows, Linux, and AIX platforms and can be used in physical, virtual, cloud, container, and big data environments – regardless of the underlying storage technology. Administrators perform all policy and key administration through the CipherTrust Manager. Encryption takes place on the server, eliminating bottlenecks that plague legacy, proxy-based solutions. Performance and scalability are further enhanced by leveraging cryptographic hardware modules that are built into such modern CPUs as Intel AES-NI and IBM POWER9.

Protect data on-premises or in-cloud

Keep control of your data by managing encryption keys and access policies from your local data center for both your on-premises and cloud data, even in hybrid environment deployments.

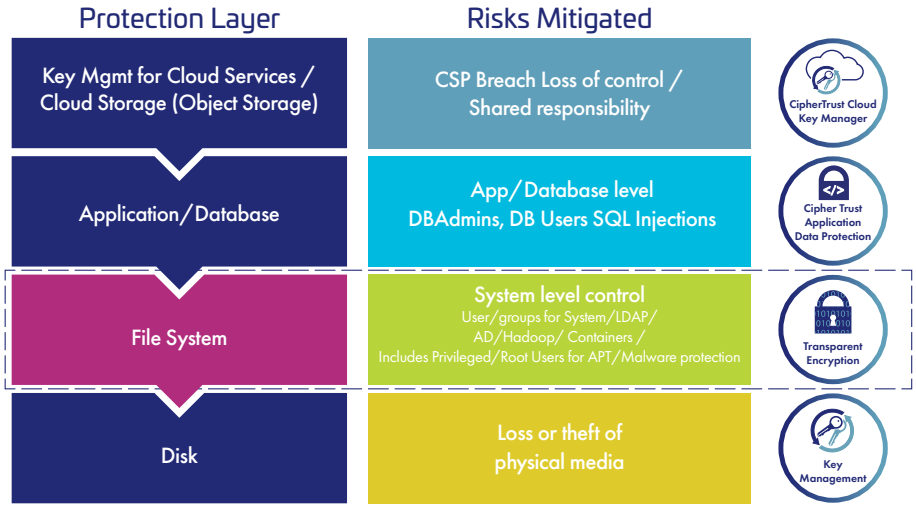


Figure 2. CipherTrust Data Security Platform – Risks and Protection Layers for Transparent Encryption

Advanced capabilities

- **Zero-downtime data transformation.** The 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.
- **Advanced access controls for big data (Hadoop).** When implemented in Hadoop environments, access controls are extended to Hadoop users and groups.
- **SAP HANA reviewed and qualified.** SAP has qualified CipherTrust Transparent Encryption with HANA v2.0 to deliver data encryption, privileged user access control, and granular file access audit logs.

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, container, and big data environments, regardless of the underlying storage technology.

Optional extensions and additions:

- **Live Data Transformation.** Perform initial encryption and data re-keying without taking applications using data stores offline. This extension is enabled with an additional license.
- **SAP HANA qualified.** CipherTrust Transparent Encryption provides a proven approach to safeguarding SAP HANA data. This solution meets rigorous security, data governance, and compliance requirements. The solution can be quickly deployed, requiring no changes to SAP HANA or the underlying database or hardware infrastructure. With the solution, organizations can encrypt SAP HANA data and log volumes and establish strong governance and separation of duties.

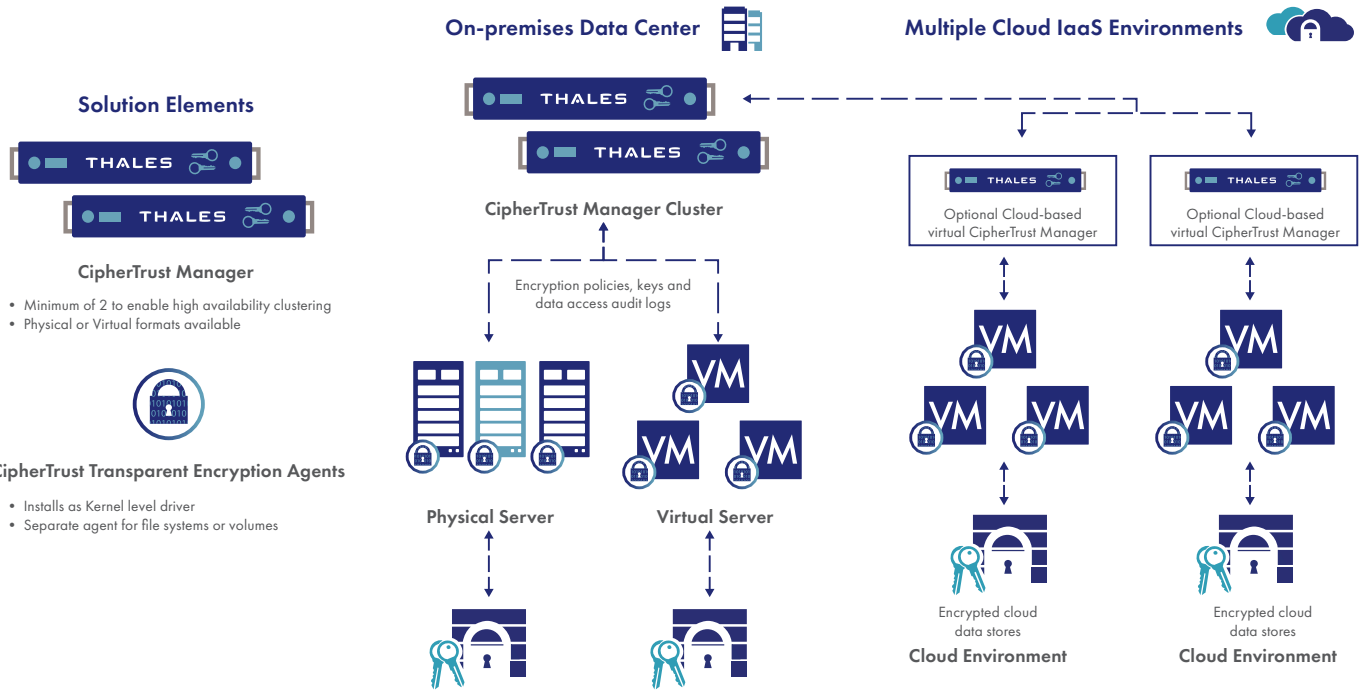


Figure 3. Basic Solution Architecture – On-premises Data Center and Multi-Cloud Environments

A simple CipherTrust Transparent Encryption deployment scenario for file system or volume data within a local data center includes:

- A CipherTrust Transparent Encryption agent deployed to the host systems or virtual machines
- Two CipherTrust Manager appliances. Two appliances are required for clustering and failover capabilities that enable solution uptime.

Additional options extend the solution's functionality.

CipherTrust Transparent Encryption Agent

CipherTrust Transparent Encryption agents are kernel level drivers that sit above file systems or volumes in the OS stack. Agents perform encryption, decryption, policy-based access control, and data access audit logging.

Policies administered by agents employ logic and fine- grained access control settings configured at the CipherTrust Manager to evaluate attempts to access protected data, and then either grant or deny access.

Controls include who is enabled to access data, what and where information is available to them, when access can be performed, and what processes are allowed to access plaintext, copy encrypted files, or even view file system metadata.

This fine-grained policy control enables operation that lets administrators and system level users perform their work (such as system backups, updates, and hardware maintenance), without having access to decrypted sensitive information.

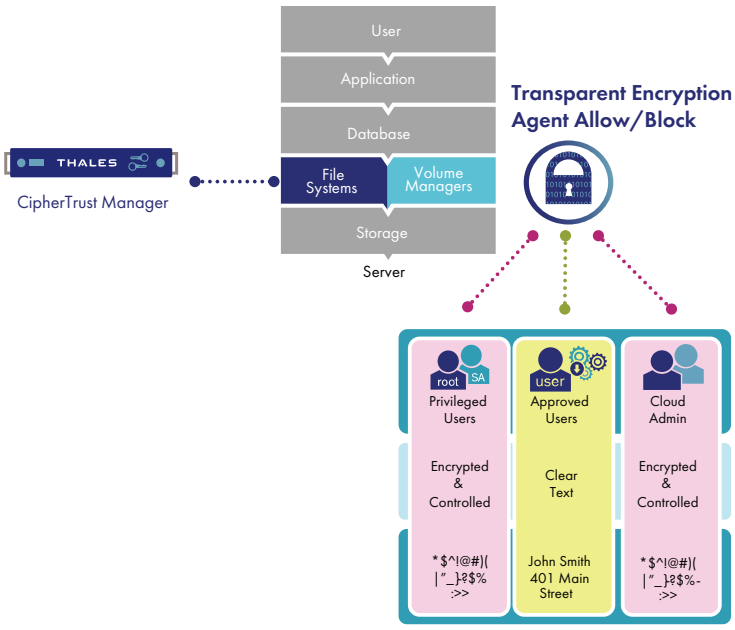


Figure 4. CipherTrust Transparent Encryption encrypts, enforces access policies, and logs all file, volume and linked cloud storage access

All activities are logged. Logs are available from the local system or the CipherTrust Manager and can be integrated with leading SIEM systems. See the section of this white paper on Security Intelligence for further detail.

Application uptime, for the solutions whose data CipherTrust Transparent Encryption protects, is supported with an easily available failover capability. Simply deploy agents at the primary and failover locations and keep encrypted data stores in sync with standard processes. When top level application failover is required, enable the same policy used at the primary location at the failover location. Sensitive information is continuously protected, and business operations continue with standard failover operation.

CipherTrust Transparent Encryption is designed to minimize impact on overall system performance. The AES-256 hardware-accelerated encryption capabilities available from modern CPUs are used by the agent regardless of the environment. AIX, Linux, and Windows deployments to physical servers, virtual environments, cloud, and even container environments all benefit from the extremely low overhead on encryption and decryption available from hardware acceleration.

Environment Support

OS Support Microsoft: Windows Server 2012, 2016, and 2019 Linux: Red Hat Enterprise Linux (RHEL), SuSE Linux Enterprise Server, AWS Linux and Ubuntu, UNIX: IBM AIX	**Big Data Support** Hadoop: Cloudera, Hortonworks, IBM NoSQL: Couchbase, DataStax, MongoDB, SAP HANA
Database Support IBM DB2, Microsoft SQL Server, MySQL, NoSQL, Oracle, Sybase, and others	**Encryption Hardware Acceleration** AMD and Intel AES-NI, IBM P9 cryptographic coprocessor
Application Support Transparent to all applications, including Documentum, SAP, SharePoint, custom applications, and more	**Agent Certification** FIPS 140-2 Level 1
File systems Supports most standard file systems for each OS – See your Thales sales representative for a complete and current listing. **Cloud Storage** Amazon AWS – EBS, EFS, and via the AWS Storage Gateway also supports S3 Standard, S3 Infrequent and S3 Glacier Microsoft Azure – Disk Storage, Azure Files	**Users and Groups** System, LDAP/AD, Hadoop and Containers

Powerful protection against root and privileged user risks

CipherTrust Transparent Encryption includes highly intelligent protection against root user attacks. The solution will log and control access based on user roles and groups (system, LDAP/AD, Hadoop, Containers), but also has additional capabilities to combat root user attacks. The root user role has the capability to both create system level accounts and to log in to other system level accounts. When root users use these capabilities to change to an account that has access to sensitive data, access to the data will still be denied if the root user is not specifically allowed access by CipherTrust Transparent Encryption policy (as defined at the CipherTrust Manager). The solution will be aware of the original login account as root and deny or allow access based on the policies for that root account.

CipherTrust Manager

The CipherTrust Manager is the common centralized management environment for all CipherTrust Data Security Platform products. It provides policy control as well as secure management and storage of encryption keys, includes a web-based console as well as CLI and REST APIs. The CipherTrust Manager is available as FIPS 140-2 compliant virtual and physical appliances.

The CipherTrust Manager also provides a unified way to manage keys for third-party platforms, such as IBM Guardium Data Encryption (GDE), Oracle Transparent Data Encryption (TDE), Microsoft SQL Server TDE, and KMIP-compliant encryption products. The CipherTrust Manager can also store and manage X.509 certificates, symmetric keys, and asymmetric keys.

Strong Separation of Duties

The CipherTrust Manager can be configured as a multi-tenant device that runs many different virtual CipherTrust Managers, which are called "domains." The CipherTrust Manager can enforce strong separation of duties by requiring more than one data security administrator to manage or change key and policy permissions. CipherTrust Manager administration can be broken into three categories: system, domain, and security. In this manner, no one person has complete control over security activities, encryption keys, or administration. Also, the CipherTrust Manager supports two-factor authentication for administrative access.

Users and groups for data security management tasks can be based on locally defined users or groups, or imported via LDAP from Active Directory or other directory services and identity management environments.

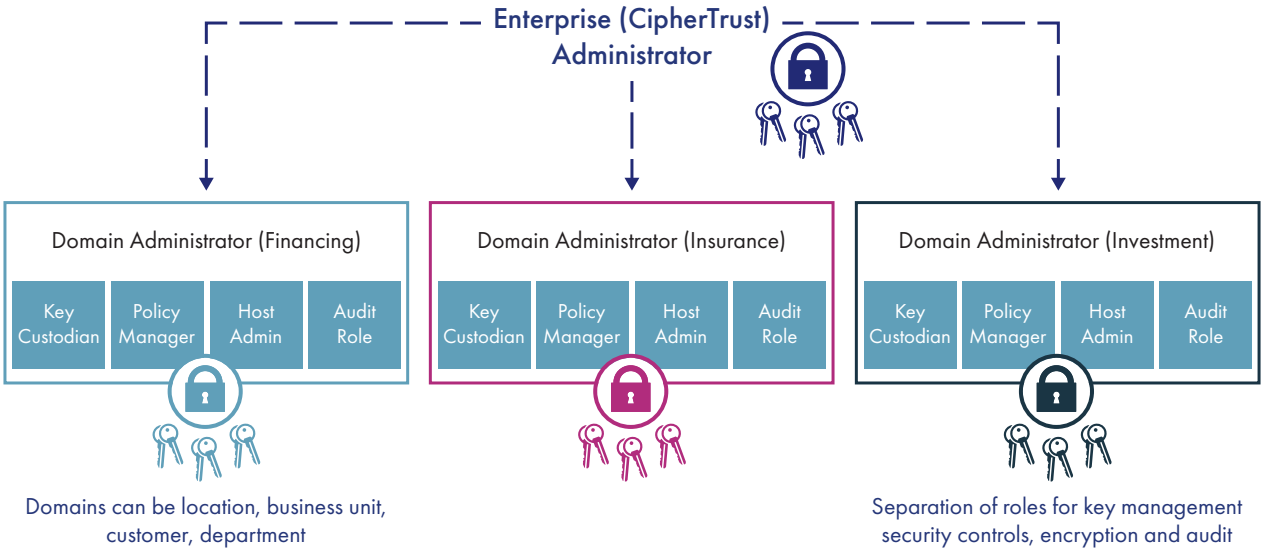


Figure 5. Multitenant Key Management and Strong Separation of Duties

To further isolate and protect sensitive data, the CipherTrust Manager and CipherTrust Transparent Encryption work in tandem to allow security administrators to create a strong separation of duties between data owners and privileged IT administrators. Users and groups used in policies for access control to data can be based on system level roles, LDAP/AD, Hadoop users/groups/zones as well as container environment users and groups.

If desired, CipherTrust Transparent Encryption can encrypt files while leaving their metadata in the clear. This capability enables IT administrators to perform system administration tasks (such as replication, backup, migration, snapshots, and system updates), without exposure to sensitive data. The CipherTrust Manager also can control basic system commands such as copy, write, and directory listings.

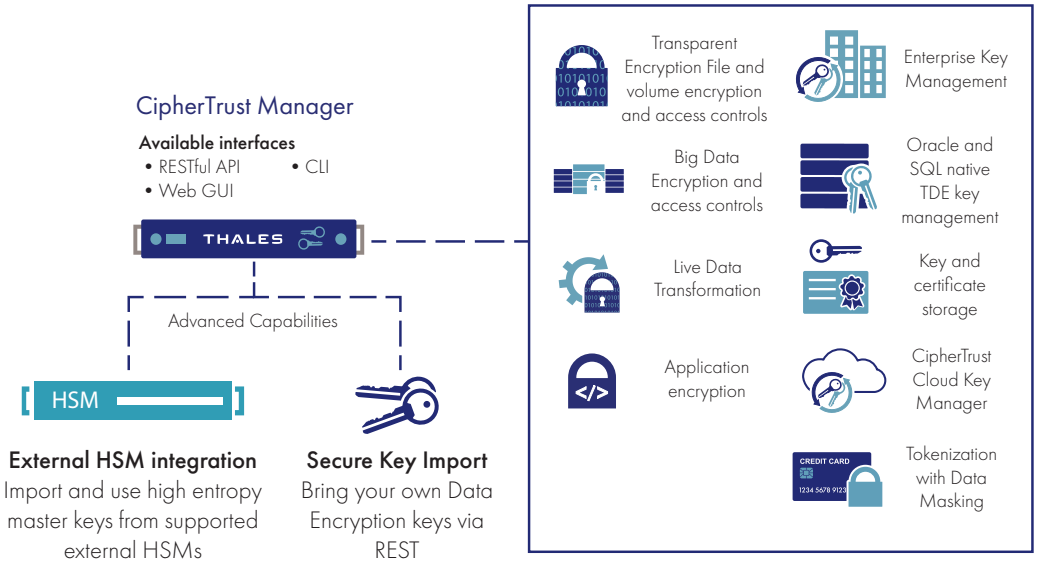


Figure 6. Centralized, integrated policy and encryption key management for all CipherTrust Data Security Platform products

CipherTrust Manager High Availability

CipherTrust Managers can be clustered for High Availability (HA), and Thales recommends this configuration for all implementations with a minimum deployment of two CipherTrust Managers. When configured for HA, one CipherTrust Manager acts as the primary and others are used for failover, scalability, or in additional locations where latency is a concern, such as a remote data center or cloud location.

All configuration settings, including changes to administrators, domains, hosts, keys, and policies, are made on the primary CipherTrust Manager, other CipherTrust Managers are read-only. Configuration changes and updates on the primary CipherTrust Manager are pushed to the other CipherTrust Managers at set intervals using replication.

APIs and interfaces

A web-based UI console and RESTful APIs are available. APIs make it possible to manage CipherTrust Manager functions remotely and are designed to operate in environments that require high levels of automation, such as service providers with cloud environments or highly automated data centers.

CipherTrust Security Intelligence

CipherTrust Transparent Encryption agents and CipherTrust Manager provide extensive logging capabilities detailing successful and attempted access attempts to protected data and the CipherTrust Manager management environment, agent interactions and key operations, as well as the actions of administrators at the CipherTrust Manager. Logs are designed to meet a range of needs for information from the solution. These include:

- Audit level information required by compliance, regulatory mandates, and best practice security reports
- Immediate insight into attempted access events by users and processes that may represent threats
- Detailed historical usage data that can be used to create baselines of expected operation from access pattern recognition

Logs are available in standard formats used by security information and event management (SIEM) systems (RFC5424, CEF and LEEF), and are available from CipherTrust Managers as well as from systems hosting CipherTrust Transparent Encryption agents. The primary CipherTrust Manager can be used as a collection point for all logs from CipherTrust Managers and CipherTrust Transparent Encryption agents if desired.

These logs provide deep visibility into data access, which can be used to alert administrators to unauthorized access attempts to protected data that may represent a threat, and to build typical access patterns when combined with other infrastructure and access information. For instance, a user that typically accesses information in small quantities from within a local network, if seen to be accessing large volumes of data from a remote location, would represent a threat that should generate an alert and be investigated.

Detailed logs include information about when users and processes accessed data, under which policies, and if access requests were allowed or denied. The logs will even expose when a privileged user leverages a command like "switch user" to imitate another user. Logs are designed to be able to easily meet the auditing requirements of compliance mandates and regulations as well by delivering the detailed evidence needed to prove to an auditor the encryption, key management, and access policies are appropriate and operating correctly.

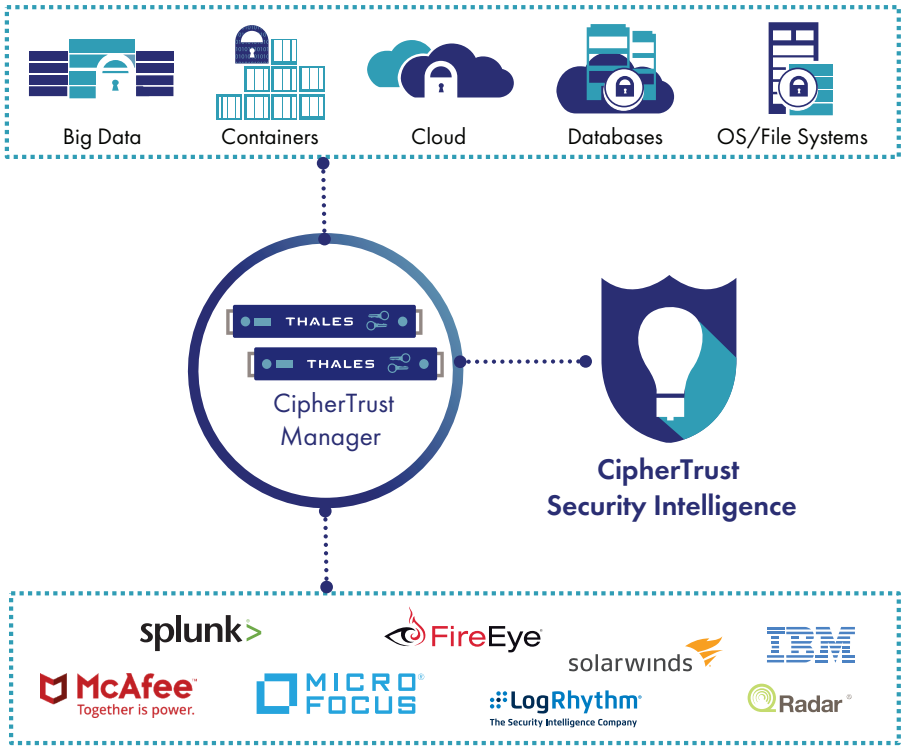


Figure 7. CipherTrust Security Intelligence

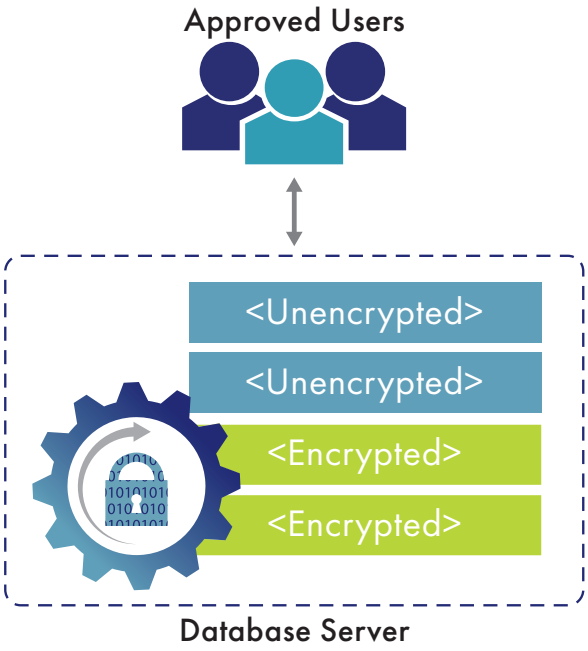


Figure 8. CipherTrust Transparent Encryption with CipherTrust Live Data Transformation Enabled

Live Data Transformation Extension

Deployment and management of data-at-rest encryption can present challenges when transforming clear-text to cipher-text, or when rekeying data that has already been encrypted. Traditionally, these efforts either required planned downtime or labor-intensive data cloning and synchronization efforts. CipherTrust Transparent Encryption Live Data Transformation Extension eliminates these hurdles, enabling encryption and rekeying with unprecedented uptime and administrative efficiency.

Zero-downtime encryption and key rotation.

Live Data Transformation delivers these key capabilities:

- Zero-downtime encryption deployments. The solution enables administrators to encrypt data without downtime or disruption to users, applications or workflows. While encryption is underway, users and processes continue to interact with databases or file systems as usual.
- Seamless, non-disruptive key rotation. Both security best practices and many regulatory mandates require periodic key rotation. Live Data Transformation makes it fast and efficient to address these requirements.

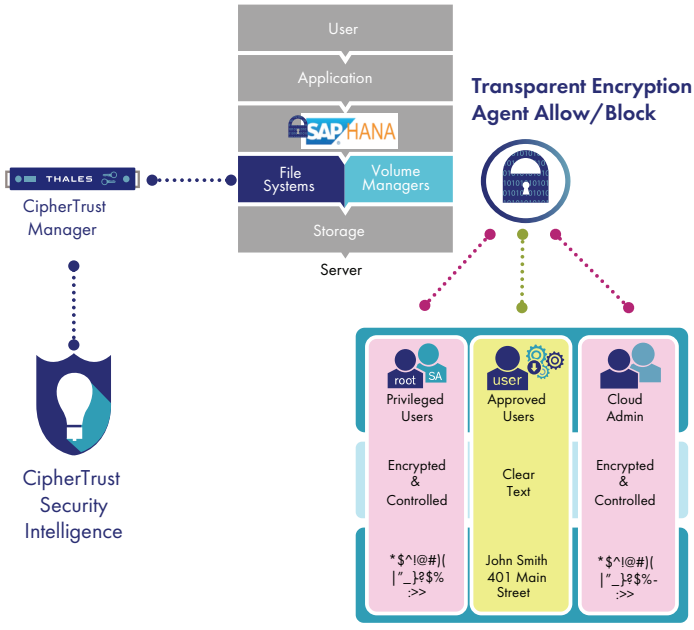
With the solution you can perform key rotation without having to duplicate data or take associated applications offline.

- Intelligent resource management. Encrypting large data sets can require significant CPU resources for an extended time. Live Data Transformation provides sophisticated CPU use and I/O rate management capabilities so administrators can balance between the resource demands of encryption and other business operations. For example, an administrator can define a resource management rule specifying that, during business hours, encryption can only consume 10% of system CPU, while on nights and weekends, encryption can consume 70% of CPU.
- Versioned backups and archives. With key versioning management, Live Data Transformation offers efficient backup and archive recovery that enable more immediate access. In a data recovery operation, archived encryption keys recovered from the CipherTrust Manager are automatically applied to an older data set. Restored data is encrypted with the current cryptographic key.

CipherTrust Transparent Encryption for SAP HANA

CipherTrust Transparent Encryption provides a proven approach to safeguarding SAP HANA data that meets rigorous security, data governance, and compliance requirements. The solution can be quickly deployed, requiring no changes to SAP HANA, the underlying database, or hardware infrastructure. With this solution, organizations can encrypt SAP HANA data and log volumes, and establish strong governance and separation of duties.

- Enforce strong data encryption on all SAP HANA data and log partitions
- Protect and control access to the SAP HANA persistence layer
- Use granular access controls to prevent privileged users and system administrators from accessing unauthorized data
- Facilitate compliance with new and existing data security mandates
- Maintain key and security policy custody on tenant/customer premises



Secure Import of Data Encryption Keys

As organizations increasingly place business-critical data within multiple cloud environments, the question of who controls the encryption keys that protect sensitive data becomes increasingly important. Enterprises prefer to control and even create the data encryption keys protecting their cloud environment data. Those with the highest levels of IT security requirements may even wish to control the creation of their in-house keys for maximum complexity, randomness, and assurance.

The CipherTrust Data Security platform provides the capability for cloud service providers and enterprises to offer multi-tenanted access to CipherTrust Managers that enables them to create and bring in data encryption keys used with CipherTrust Transparent Encryption agents rather than use the data encryption keys generated by the CipherTrust Manager. Data encryption keys can be created by a trusted hardware device (such as a Thales or third-party Hardware Security Module) or from an existing key management and creation application. Keys imported for use with CipherTrust Transparent Encryption agents can then be used as needed with policies created within the CipherTrust Manager.

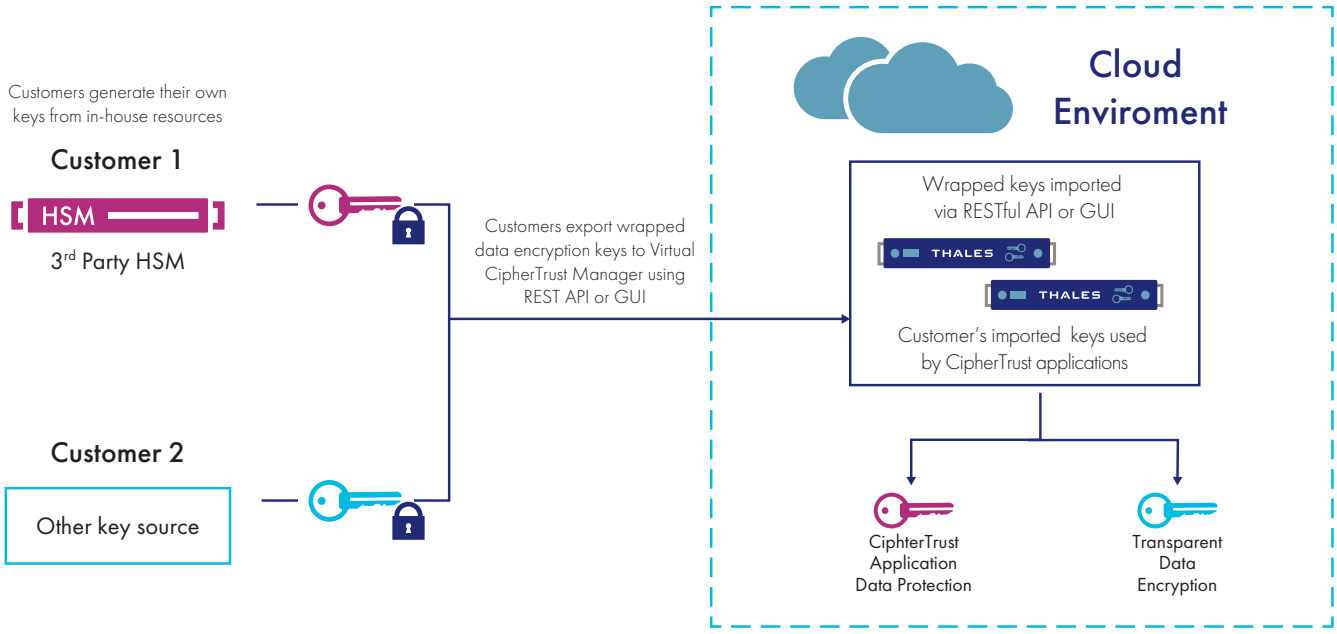


Figure 9. Maintain complete control of encryption keys, even within multi-tenant cloud environments

Use cases

Databases and Unstructured Files – Across Data Centers and Cloud Environments

As organizations continue to grow their infrastructure and data sets, they have to deal with a mix of in-house and cloud-based data assets and applications. Regardless of where this data is located, it requires the same level of data security and protection. CipherTrust Transparent Encryption enables enterprises to choose their implementation mode for data security based on their risk tolerance, compliance, and privacy requirements.

Most enterprises will opt for a solution that includes managing and controlling from their local data center encryption keys and access policies for both local data center resources and cloud environments. This approach keeps control of keys firmly within the enterprise, eliminating the risk of remote legal access or compromise at the cloud provider. Enterprises that are "all in" the cloud and make no use of local data center compute resources may opt for a cloud-based deployment of key and policy management. Such organizations can either co-locate cloud key management in the same cloud with data protected by CipherTrust Transparent Encryption, using a secondary cloud environment for the CipherTrust Manager to provide a greater degree of separation and lower risk, or use a co-location or hosting provider for hardware versions of CipherTrust Managers. All of these scenarios are easily supported with CipherTrust Transparent Encryption by locating physical or virtual CipherTrust Managers in local data centers, co-location vendors, hosting solutions, or cloud environments as needed.

Regardless of the deployment model, a typical database protection scenario includes a CipherTrust Transparent Encryption agent deployed to database servers with a simple policy – a signed database process and the database user are allowed cleartext access to the protected data store, all others will only see file metadata and ciphertext. This effectively shields the database access from compromise by root and privileged user-based attacks, local system, and LDAP users and groups while also meeting compliance and best practice requirements for safeguarding the data set with encryption.

For larger data sets, customers will typically purchase the Live Data Transformation extension to CipherTrust Transparent Encryption, enabling immediate encryption of the database without taking critical applications offline and periodic rekeying to meet compliance and best practice requirements without downtime.

We will use a directory for a typical unstructured file system protection example. The CipherTrust Transparent Encryption agent is deployed to the server with separate policies for LDAP/Active Directory user groups. For instance, allowing only finance department members to access critical accounting data, HR to access confidential employee information, and Engineering to access development documents. Each data store section is encrypted with an individual key by policy, effectively limiting the access to only those who require it for their work.

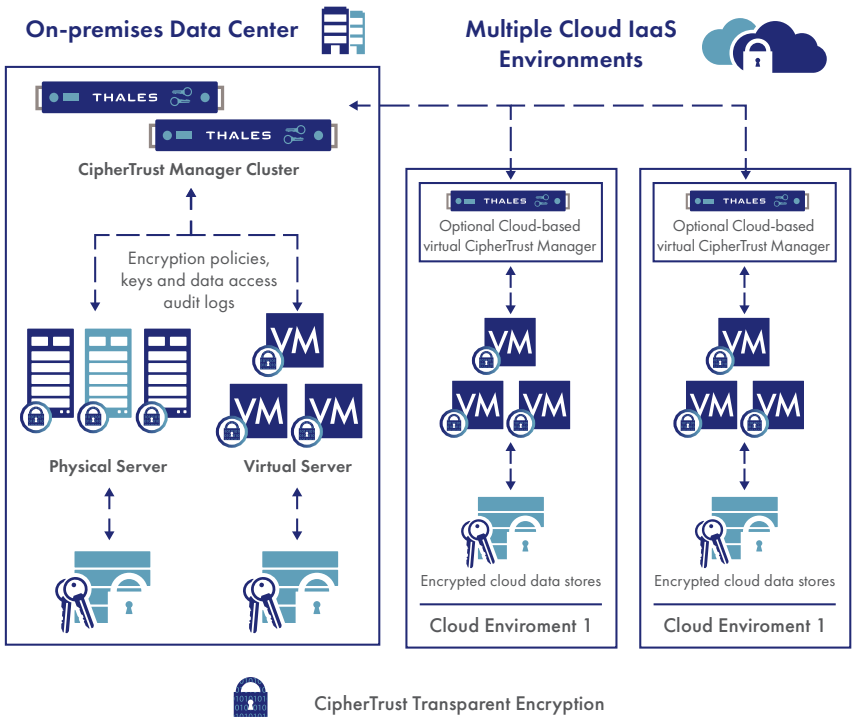


Figure 10. Fully integrated enterprise on-premises and cloud enviroment deployment

Big Data

With nearly every enterprise embracing big data environments, and with large numbers of these environments implemented in the cloud, the security of the sensitive data within the data lake, source data environments, and the reports that hold high-value correlated results have become an insistent concern.

CipherTrust Transparent Encryption safeguards this information. The solution can be used to protect data at the file system level within compute notes (and underlying storage), source data locations, as well as the repositories used for logs and reports. And, this protection extends beyond the system level users/ groups and LDAP/AD users and groups that are enforced by CipherTrust Transparent Encryption on a typical server. The solution also enforces policy-based encryption, access controls and data access logging by Hadoop users, groups and zones. This capability provides further protection against privileged users within the big data lake or users within the environment.

A typical deployment includes agents installed on compute nodes, source data servers, and servers accessing log/report repositories. Data is encrypted throughout the environment with appropriate access policies and data access logging controls provided by the CipherTrust Manager. Further, the use of hardware encryption capabilities in underlying compute infrastructure results in minimal overhead from encrypt/ decrypt operations. This makes it possible to use the solution even where speed and compute capability are critical.

Further, Thales works with leading big data environment vendors as a partner to ensure solution capability and operation. At the time of this writing, these partners include DataStax, MongoDB, Teradata, IBM, Cloudera, Couchbase, SAP HANA, and Hortonworks.

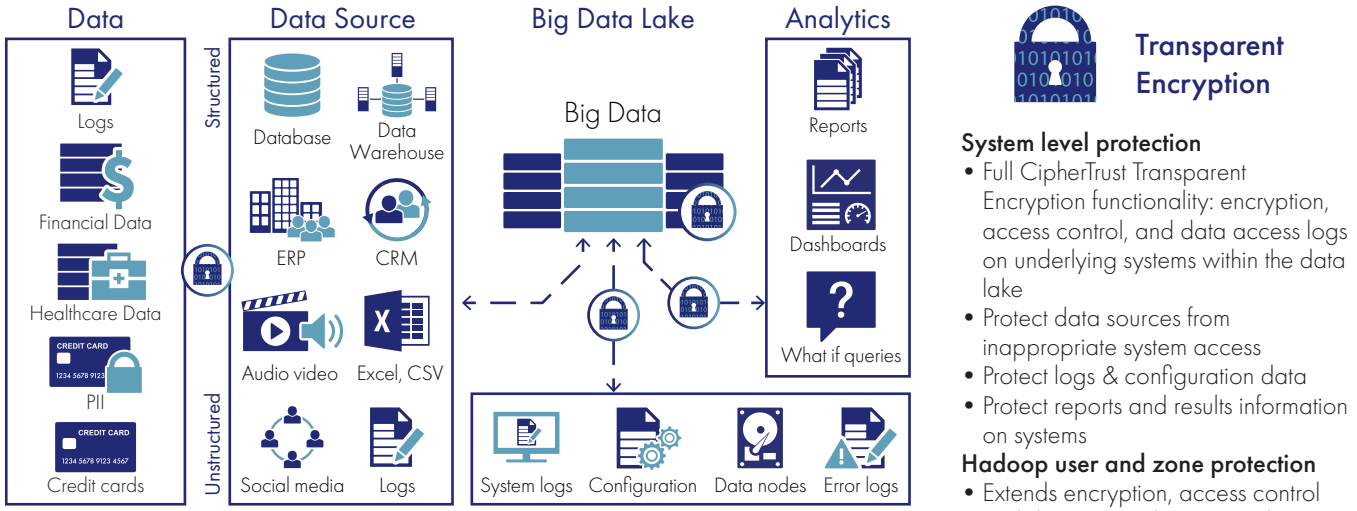
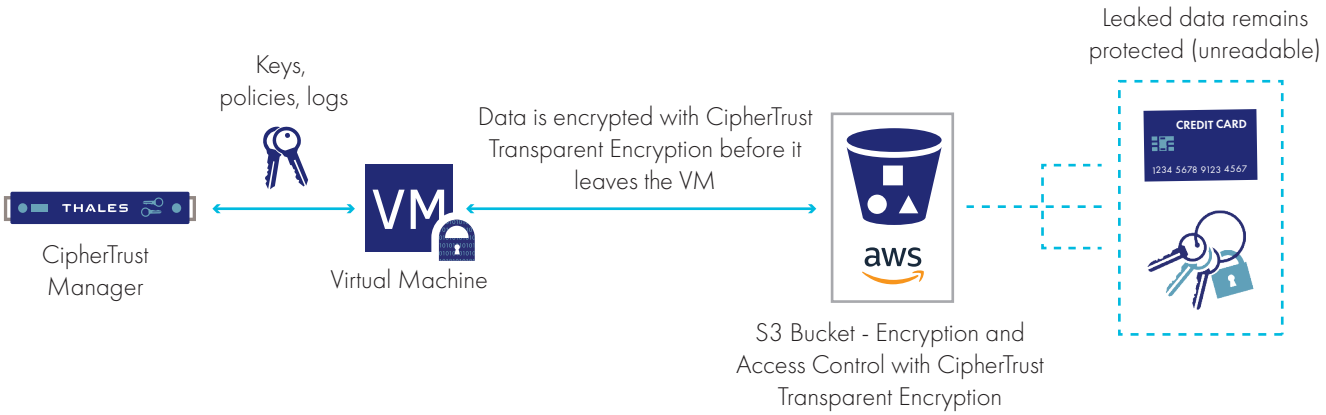


Figure 11. Protecting data within big data environments using CipherTrust Transparent Encryption

Advanced data protection for Amazon S3

As organizations increasingly use Amazon S3 cloud storage as part of their implementation strategy, as well as for backups and failover environments, they need to protect data within these S3 buckets just as they would if the storage were located within their own data centers.

With advanced data protection for Amazon S3, organizations can apply transparent encryption and access controls to sensitive data in S3 buckets. The CipherTrust Trasnparent Encryption solution encrypts unstructured files, semi-structured data, or structured databases before they are written to Amazon S3 buckets. This assures that the data is always encrypted in-flight, for example from on-premises hosts or Amazon EC2 instances to the S3 buckets. Decryption only occurs once the data is on the server where it will be used. In addition, CipherTrust Transparent Encryption protection for Amazon S3 features enhanced granular access controls, which, when deployed with custom AWS IAM policies, can enforce additional access controls to limit S3 access only to hosts running the CipherTrust Transparent Encryption for Amazon S3 agent.



Key features of CipherTrust Transparent Encryption for Amazon S3 include:

- **Transparent to applications and Amazon S3 administrators.** Encryption and access controls are completely transparent to applications while Amazon S3 administrative procedures remain unchanged after software agent deployment. The encryption offered by this solution is independent of Amazon S3 server-side encryption.
- **Continuous protection even with misconfigured S3 buckets.** Continuously enforces policies that protect against unauthorized access by users and processes even in the case of Amazon misconfigurations. Data access to protected S3 buckets is tracked through detailed audit logs.
- **Granular controls.** Applies granular, least-privileged user access policies that protect sensitive data in S3 buckets from external attacks and misuse by other privileged users. Security administrators can set up access controls on bucket creation, deletion, and enumeration, as well as for object creation, deletion, and updates. Optional S3 server-side access controls can be enabled with custom IAM policies to restrict S3 bucket access only to hosts configured with CipherTrust Transparent Encryption.
- **Strong data security.** Employs strong, standards-based encryption protocols, such as Advanced Encryption Standard (AES) for data encryption and Elliptic Curve Cryptography (ECC) for key exchange. TLS 1.3 and other NIST recommendations adopted to enforce strong key and data security. The agent is FIPS 140-2 Level 1 validated. The encryption keys are always created and managed by the CipherTrust Manager, a FIPS 140-2 Level 3 compliant appliance.
- **Security intelligence logs.** Identify and stop threats faster with detailed data access audit logs that produce an auditable trail of permitted and denied access attempts from users and processes, delivering unprecedented insight into file access activities.

Summary

The urgent need for data-at-rest encryption continues to grow. Compliance requirements proliferate. Digital transformation expands attack surfaces. And every day we see new internal and external threats to critical IP, PII, customer and citizen information, and more. With CipherTrust Transparent Encryption, organizations can secure their file and volume data wherever it is stored in a wide range of environments and use cases. And, CipherTrust Transparent Encryption is an integral part of a single platform solution that provides comprehensive data-at-rest security across the entire enterprise. The solution helps organizations address their security mandates while minimizing costs and administrative efforts.

Appendix: Performance benchmarks

Intel®, AMD, and PowerPC processor family all include hardware accelerated encryption capabilities that are leveraged by CipherTrust Transparent Encryption agents. For Intel, this includes Intel® Data Protection Technology with Advanced Encryption Standard New Instructions (AES-NI). AES-NI accelerates AES encryption and has been optimized for fast throughput and low latency.

CipherTrust Transparent Encryption uses AES-NI instructions for hardware-based acceleration of data encryption and decryption. In fact, CipherTrust Transparent Encryption has a proprietary encryption engine that is designed to take full advantage of the parallelism that can be achieved with multi-core processor chipsets and it specifically leverages the pipelining capabilities of AES-NI. As a result, the solution delivers the maximum performance possible.

In addition to leveraging hardware-based encryption capabilities, CipherTrust Transparent Encryption is tightly integrated with, and optimized for, each supported operating system kernel. Consequently, CipherTrust Transparent Encryption leverages the latest features available for every platform supported, rather than being coded to a lowest common denominator across multiple platforms. With each new release, Thales continues to add new capabilities that enable the solution to exploit the latest operating system features.

For many applications, the performance overhead that CipherTrust Transparent Encryption introduces is negligible. However, as loads associated with input/output (I/O) increase, there will be increased overhead associated with encryption. Even with demanding, I/O heavy applications, such as databases or big data processing, CipherTrust Transparent Encryption generally introduces less than 10% overhead.

One example can be seen in the chart below. In this example, the Yahoo Cloud Serving Benchmark (YCSB) was run against MongoDB 4.0.3, with the WiredTiger storage engine running on top of CipherTrust Transparent Encryption. YCSB is a generally available open source framework that has a common set of workloads for evaluating the performance of different "key-value" and "cloud" serving stores. The workload was configured so that less than one-half of the data set could fit in memory, causing a heavy I/O load. As the chart illustrates, CipherTrust Transparent Encryption only introduced minimal overhead.

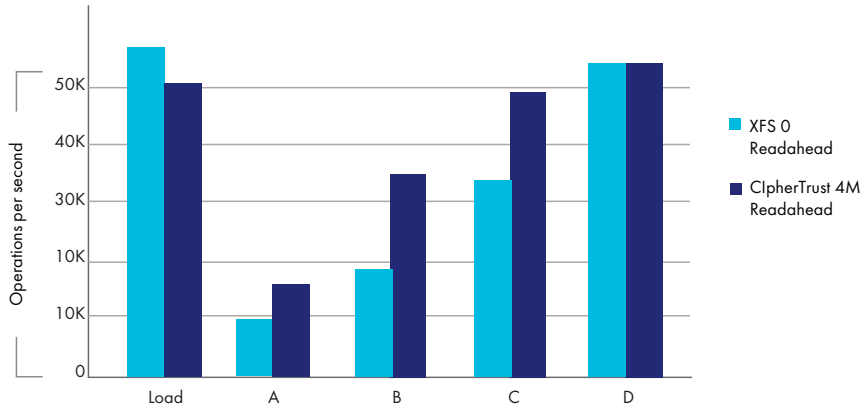


Figure 12. Even when testing in a scenario with a heavy I/O load, CipherTrust Transparent Encryption introduces minimal performance overhead.

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 <