Trusted Cyber Technologies

THALES
Building a future we can all trust

Avoiding Amazon S3 Data Leaks with Scalable Encryption and Access Controls

White Paper

Contents

Securing sensitive data in the cloud

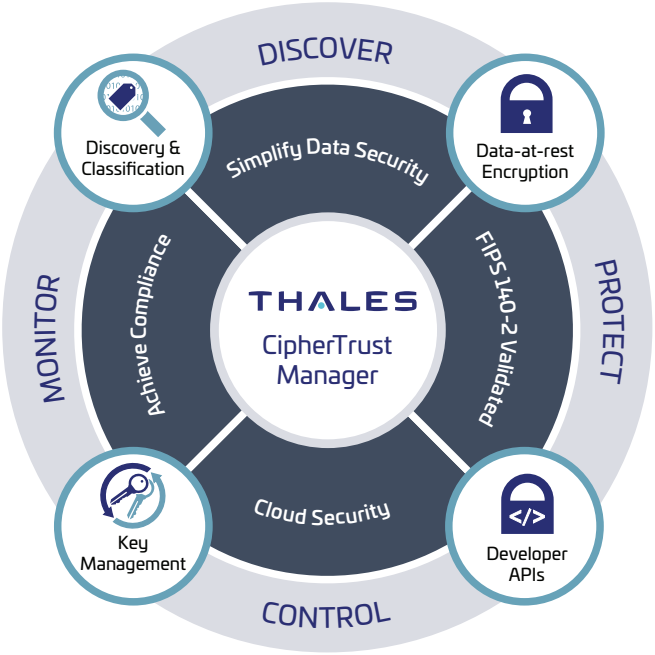
Cloud computing is transforming the way enterprises, government agencies, and small businesses manage their company data. Elastic public cloud services are enabling agile, cost-effective methods to run business-critical applications and store information. And, while some enterprises aren't yet ready to let go of the traditional on-premises data center, they are exploring and evaluating all available options.

Amazon Simple Storage Service (S3), one of the leading cloud storage solutions, is used by companies all over the world to power their IT operations for a variety of use cases. Amazon S3 buckets have become one of the most commonly used cloud storage repositories for everything from server logs to customer data. However, poorly configured S3 buckets have been the cause of a large number of data breaches. According to 2019 Verizon Data Breach Report, misconfiguration of cloud platforms accounted for 21 percent of breaches.[1] Amazon does provide a range of security services and features that its customers can use to secure their assets. However, the cloud service provider places responsibility for protecting the confidentiality, integrity, and availability of data in the cloud, and for meeting specific business requirements for information protection, in the hands of its customers.

To fully secure data in an untrusted and multi-tenant cloud environment, organizations must maintain complete governance and control of their data. Thales simplifies securing S3 objects and helps achieve compliance with data security regulations with CipherTrust Transparent Encryption. The CipherTrust Transparent Encryption agent operates seamlessly on objects in S3 delivering transparent and automated encryption of sensitive data stored in Amazon S3 buckets without any changes to applications, databases, infrastructure, or business practice.

The CipherTrust Data Security Platform from Thales

CipherTrust Transparent Encryption for Amazon S3 is part of the CipherTrust Data Security Platform, which efficiently enables data-at-rest security across the entire enterprise, regardless of where data is used. Built on a single extensible infrastructure, the CipherTrust Data Security Platform products can be deployed as needed while sharing a common, scalable policy control and key management environment. In addition to CipherTrust Transparent Encryption, the CipherTrust Data Security Platform delivers capabilities for application-layer encryption, tokenization, dynamic data masking, cloud, and on-premise key management. These capabilities enable organizations to safeguard and control access to data regardless of where it is stored or used, meeting requirements for compliance, regulatory mandates, data privacy standards, and best practices with a single infrastructure and management environment.



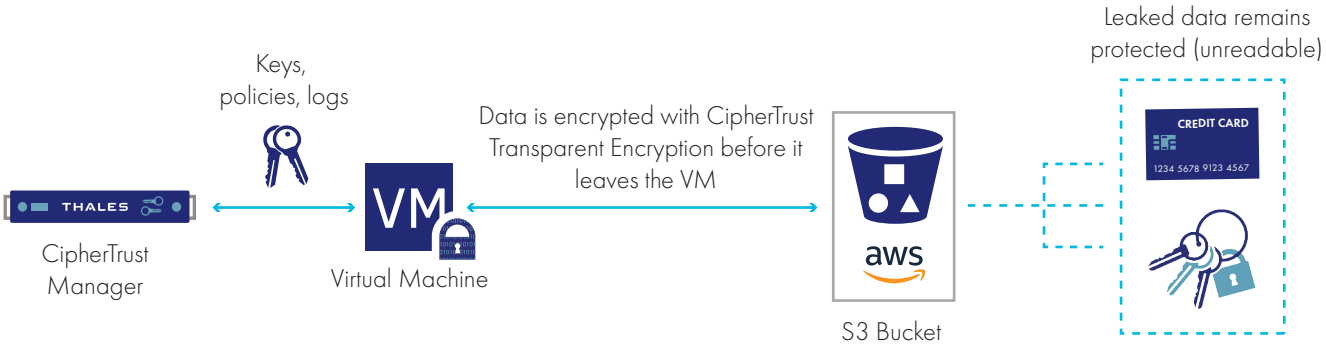
1 https://threatpost.com/verizon-dbir-espionage-c-suite-cloud/144486/

Advanced data protection for Amazon S3 with CipherTrust Transparent Encryption

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. Implementation of the encryption software is seamless keeping both business and operational processes working without changes even during deployment and roll out. The FIPS 140-2 Level 1 software agent works in conjunction with the FIPS 140-2 (Level 2 or Level 3) validated Manager, which centralizes encryption key and policy management for the CipherTrust Data Security Platform.

As organizations increasingly use Amazon S3 cloud storage as part of their implementation strategy, as well as backups and failover environments, they now need to protect data within these S3 buckets just as they would if the storage were located within their own data center. With advanced data protection for Amazon S3, organizations can apply transparent encryption and access controls to sensitive data in S3 buckets. The solution encrypts unstructured files, semi-structured data, or structured databases before it is 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 from hosts running the CipherTrust Transparent Encryption for Amazon S3 agent.

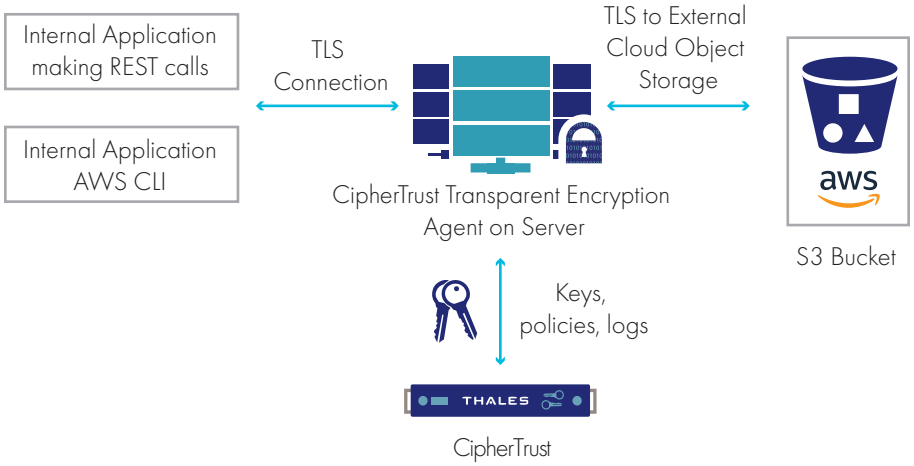
CipherTrust Transparent Encryption agent and CipherTrust Manager (DSM) provide extensive logging capabilities detailing successful and attempted access to protected data. These logs can inform of unusual or improper data access and accelerate the detection of insider threats, hackers, and Advanced Persistent Threats (APT) that have bypassed perimeter security. CipherTrust Security Intelligence logs easily integrate with all leading Security Intelligence Event Management (SIEM) tools using their pre-defined CipherTrust dashboards and reports. To further isolate and protect sensitive data, DSM administrators can set policies to encrypt data at the host prior to sending it out, block devices or S3 buckets, granting access only to authorized individuals or groups. Once an S3 bucket is guarded, any file deposited into this protected bucket is automatically encrypted and the data inside is rendered useless in the event of unauthorized access. CipherTrust Transparent Encryption for Amazon S3



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 his 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 protects 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 from 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 DSM, a FIPS 140-2 Level 3 validated 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.

CipherTrust Transparent Encryption for Amazon S3



CipherTrust Transparent Encryption deploys a secure and hardened TLS proxy to intercept HTTPS traffic originating from the server with the CipherTrust agent to guard S3 buckets. After the agent intercepts a set of specific S3 operations (such as GET, PUT, DELETE), the access controls ensure that the local user and application is authorized with the proper read or write permissions for the object or bucket as per the CipherTrust Transparent Encryption policy in use. The result is that the agent encrypts the HTTPS data buffers inline, provides access controls, secure key exchange and handles the authorized encryption/decryption actions accordingly.

CipherTrust Manager with CipherTrust Transparent Encryption

The CipherTrust Manager is the centralized management component for all CipherTrust Data Security Platform products. The appliance provides policy controls as well as secure encryption key management and storage. It includes a Web-based console as well as CLI, and REST APIs, and is available as FIPS 140-2, and Common Criteria certified virtual and physical appliances.

Available appliance form factors include:

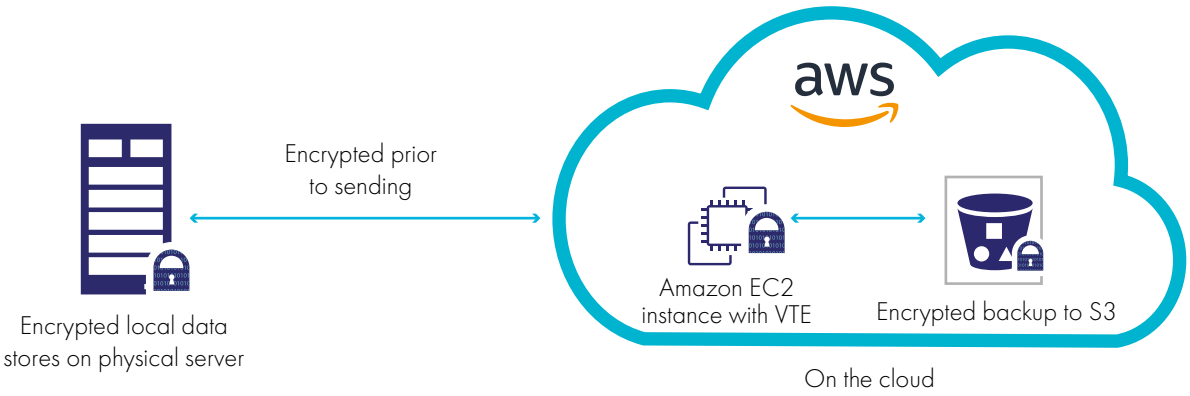
- FIPS 140-2 Level 1 virtual appliance
  - The virtual appliance is available in VMware ESXi, Microsoft Hyper-V, Linux KVM, Amazon Web Services AMI, and Azure compatible form factors
  - Supports FIPS 140-2 Level 3 root of trust from external HSMs, such as Thales TCT Luna T-Series HSM.
- FIPS 140-2 Level 2 hardware appliance
  - Supports FIPS 140-2 Level 3 root of trust from external HSMs, such as Thales TCT Luna T-Series HSM.
- FIPS 140-2 Level 3 Hardware appliance - includes an integrated HSM

The physical appliance is appropriate for your on-premises locations to manage encryption agents worldwide, across any cloud provider and for servers at remote sites.

Sample Use Cases

Encrypting data between on-premises physical server and Amazon EC2 and S3 storage

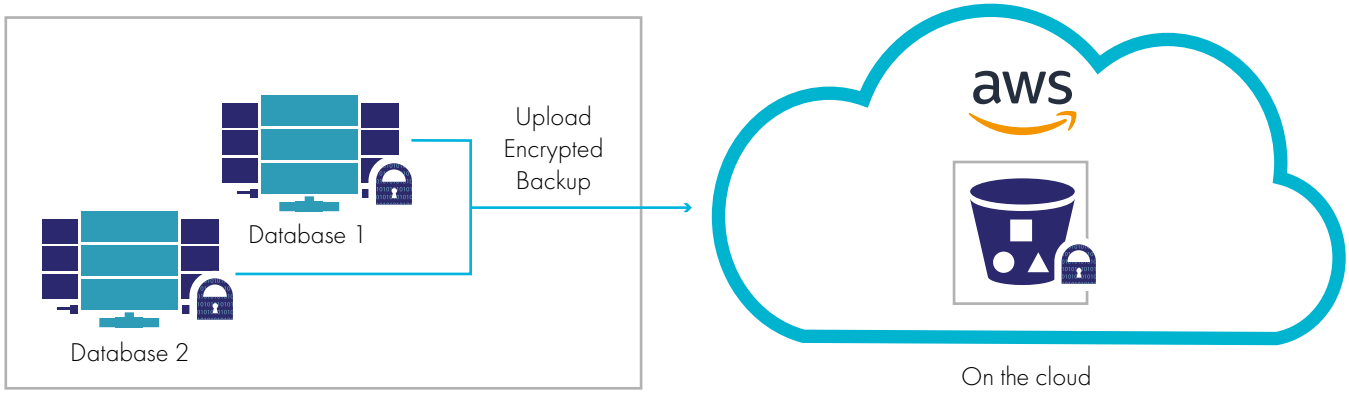
With CipherTrust Transparent Encryption, organizations can apply transparent encryption to data in Amazon Elastic Compute Cloud (EC2) and S3 environments. The solution can be used to securely transfer encrypted data between an on-premises physical server and Amazon Cloud Storage. Organizations can lock down sensitive information, including: application data (configs, passwords, logs), database data (data files, backups), data in folders (media files, images and documents, such as intellectual property and human resources or payroll files), and data in Hadoop implementations. CipherTrust Transparent Encryption is used to protect files on the physical server. The backups from the physical server host to EC2 and S3 buckets can also be encrypted using CTE for S3. Access control policies deployed during backup can ensure that only an authorized backup administrator can perform this backup while disallowing unauthorized users (including root). The same access control policies ensures only the authorized backup administrator can restore the backed-up data from S3 buckets.



Encrypting MySQL Database Backups

MySQL is a well-known open source database supported on a variety of operating systems including Linux. MySQL backups to Amazon S3 is a popular use case. A backup administrator runs the mysqldump utility to dump the database data into a local backup image, after which the backup image is uploaded to an Amazon S3 bucket using the awscli utility.

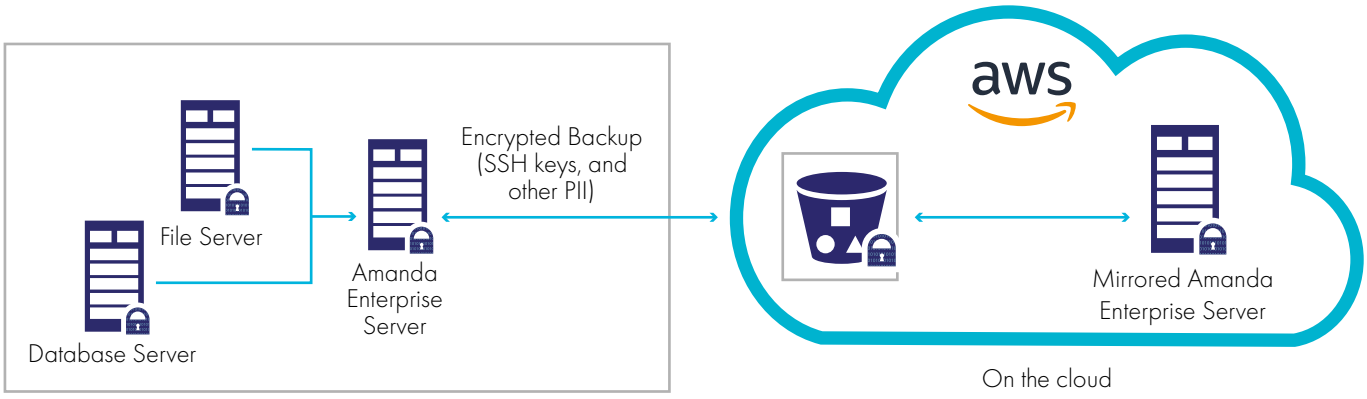
CipherTrust Transparent Encryption is used to protect MySQL system and data directories. The backups from the MySQL server host to S3 buckets can also be encrypted using CTE for S3. The awscli backup operation includes CipherTrust Transparent Encryption for Amazon S3 specification to apply encryption and access controls prior to image upload to a S3 bucket. Access control policies deployed during backup can ensure that only an authorized backup administrator can perform this backup while disallowing unauthorized users (including root). The same access control policies ensures only the authorized backup administrator can restore the backed-up MySQL images from S3 buckets.



Encrypting Amanda Backups

Amanda is an open source backup product that allows administrators to issue backup and restore operations from a centralized server with multiple host clients. Amanda supports various backup media targets with recent support for Amazon S3 targets, and is optimized to store massive amounts of unstructured data like text or SSH keys. During backups, the Amanda clients send data from source volumes to be backed up by the Amanda server. CipherTrust Transparent Encryption can be configured on the Amanda server host for both encryption and access controls when deploying Amazon S3 backup targets. This is in addition to Amanda client hosts that may also be configured to protect their data with CTE. Access controls can be applied for example, to restrict bucket access and encryption only for Amanda backup users and root users. (Note: superuser privileges are required to run restore Amanda commands like 'amrecover').

Additional Amazon S3 server side access controls can be applied with a custom IAM based role specific policy for CipherTrust Transparent Encryption to restrict S3 bucket accesses from only hosts configured with the Transparent Encryption software agent.



Amanda server host running on-prem or in cloud

Summary

Most organizations are using Amazon S3 to store sensitive data, secrets, and intellectual property. The storage is simple to deploy, but incredibly difficult to secure, as proven by the regular data leaks from Amazon S3 that are reported in the news with disturbing regularity. With CipherTrust Transparent Encryption's support for Amazon S3, organizations can ensure that volumes of data stored in the cloud are safe and comply with the strictest security regulations.

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 www.thalestct.com

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