Cloudian HyperStore Security Features

Cloudian® HyperStore® is a software-defined object storage platform that provides a multi-tenant data store for unstructured data. As well as being a massively scalable storage solution, HyperStore also provides the following security features:

Enterprise Data Protection

Cloudian HyperStore offers true enterprise data protection. With replication factors and the ISA-L Erasure Coding, Cloudian HyperStore optimizes storage protection for all data objects. Data protection and resiliency choices are flexible, enabling efficient storage redundancy to meet your specific business needs.

Secure Multi-Tenancy

Advanced identity and access-managed features allow system administrators to provision and manage groups and users, define specific classes of service for groups and users, and configure billing and charge-back policies. Multiple credentials per user are also supported. Configurable group and user level QoS rate limits ensure groups and users do not exceed storage quotas and allows for multi-access without throttling bandwidth and affecting other tenants.

Data Spill Protection

Cloudian HyperStore Secure Delete handles data spills while exceeding the NIST Special Publication 800-88-r1. Secure Delete can be set for “always on” or “always off”. When a delete occurs, Secure Delete overwrites all blocks on all nodes that contain the object — with a method that exceeds the NIST 800-88 mandate of 0’s written three times — and then the file is deleted from disk. The Secure Delete process can be audited and verified by examining delete transactions in cloudian-hyperstore-request-info.log.

Data-at-Rest and Data-in-Flight Encryption

Data-at-Rest

The HyperStore system encrypts the actual data, not the drives. Server-side encryption (SSE) uses AES-256 encryption to protect data-at-rest. Several methods of real data at rest encryption are supported:

a. Encryption using a HyperStore system-generated encryption key (SSE)

b. Encryption using a customer-provided encryption key (SSE-C)

c. Encryption using encryption keys managed by the Amazon Web Services Key Management Service (AWS KMS)

d. Encryption using encryption keys managed by a Gemalto KeySecure KMS (KMIP/OASIS coming soon)

Like Amazon S3, the Cloudian HyperStore system supports data encryption to protect the confidentiality of data at rest. The Cloudian HyperStore system can perform the encryption, and subsequent decryption, upon object retrieval. This is performed with a system-generated encryption key (regular SSE) or a customer-provided encryption key (SSE-C). The object upload and download requests must be submitted to the system via HTTPS, not regular HTTP. The system does not store a copy of the encryption key. The user is responsible for managing the SSE-C encryption key.

If an object is uploaded to Cloudian HyperStore system and encrypted with a user-provided key, the user will need to provide that same key when later requesting to download the object. HyperStore also supports the option of using a third-party Key Management System to generate and manage the encryption key (KMS). Encryption can be managed very granularly—either at a bucket level or down to an individual object.

SECURITY FEATURES & BENEFITS

Cloudian HyperStore makes it easy to build fully-featured, S3-compliant cloud storage, on-premises.

It is available as stand-alone software or as Cloudian HyperStore appliances. Cloudian HyperStore combines security functionality, availability, system management control, monitoring capabilities, and reporting.

HyperStore provides a host of security features, including:

- Data protection
- Multi-tenancy
- Data spill protection
- Authentication
- WORM
- IAM access policies
- Encryption

Cloudian’s highly efficient storage and seamless data management lets users securely store, protect, and access their data where they want it, when they want it, and to protect their data both in their private and hybrid clouds.

EAL2 Common Criteria CERTIFIED

FIPS Level 1 Validated 140-2

Data-in-Flight

The HyperStore system supports TLS 1.2 and 1.3 protocols which allows for encrypted communications between HyperStore and S3 Clients. HyperStore uses HTTPS connections with either a 3rd party CA certificate or a self-signed certificate.

WORM

HyperStore supports applying a Write Once, Read Many (WORM) policy at the bucket level via an advanced S3 extension. When a WORM policy is implemented for a bucket, objects in the bucket cannot be altered or deleted through HyperStore S3 interfaces until the object age exceeds a specified retention period.

Cloudian has engaged independent 3rd party agencies to assess Cloudian HyperStore for compliance with:

1. Securities and Exchange Commission (SEC) Rule 17a-4(f)
2. Financial Industry Regulatory Authority (FINRA) Rule 4511
3. IDW PS 880 auditing standard

AD/LDAP Authentication

HyperStore supports integration with one or more external Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) systems to authenticate and allow access to the Cloudian Management Console with secure login credentials. This feature is implemented on a per-group basis and the system supports different groups using different AD or LDAP servers for authentication, or all LDAP-enabled groups leveraging the same LDAP server.

Identity Access Management (IAM)

HyperStore provides selective support for the Amazon Identity and Access Management (IAM) API. This support enables each HyperStore user, under his or her HyperStore user account, to create IAM groups and IAM users. The HyperStore user can then grant IAM user permissions to perform certain actions (i.e. reading or writing objects in a bucket or buckets). As with Amazon, all S3 object data created by IAM users belongs to the parent HyperStore user account (otherwise known as the "root" account). IAM users can be deleted by their HyperStore parent user without any S3 object data being deleted.

The HyperStore IAM Service supports extensions to the IAM API that allow for role-based access control (RBAC) for read-only HyperStore administrative functions. The extensions take the form of additions to the list of valid values that can be specified by the "Action" request parameter in a request to the IAM Service. The supported Actions vary by the role of the requester: the IAM Service allows a HyperStore system administrator to execute a wider range of Actions than a group administrator or a regular user.

Security Certifications

Common Criteria (CC) Certification

Cloudian HyperStore version 7.2 is Common Criteria certified with EAL2 designation. At this time, HyperStore is one of two object storage platforms meeting this requirement.

What is Common Criteria?

Common Criteria (CC) is the internationally recognized standard (ISO/IEC 15408) guidelines and framework for evaluating security features and capabilities of Information Technology (IT) security products. 30 countries (including the U.S.) have signed the Common Criteria Recognition Act (CCRA).

Why does it matter?

The use of CC certification helps customers to be sure that the products they are buying have been evaluated and that the vendor's claims have been verified by a vendor-neutral third party. Having a CC certification validates that the product evaluated and certified meets an agreed-upon security standard for government deployments. Cloudian customers have the assurance that the process of specification, implementation, and evaluation of the HyperStore software solution was conducted in a thorough and standard manner.

- Certification name: Common Criteria for Information Technology Security Evaluation
- Certification level: Evaluation Assurance Level 2 (EAL2)

  The EAL2 designation indicates the product has been structurally tested to meet the outlined security criteria.
- Certification Date: Certification approval was obtained on June 25, 2019. Approved certifications are valid when using HyperStore 7.2 software.

FIPS 140-2 Validation

Cloudian has recently completed its validation, and NIST awarded a FIPS 140-2 Level 1 certification for our implemented Cloudian cryptographic module integrated as part of Cloudian's HyperStore object storage platform. The Federal Information Processing Standard (FIPS) Publication 140-2 (FIPS PUB 140-2) is a U.S. government computer security standard used to approve cryptographic modules.

NIST awarded Cloudian's FIPS 140-2 Level 1 validation using the Cloudian cryptographic module integrated into the HyperStore 7.2.x software and later release versions. Being FIPS validated ensures that the encryption methods used by Cloudian within the HyperStore have been independently reviewed and tested to provide assurance that industry-standard security requirements are met before the solution is deployed.

The Cloudian NIST validation certificates are available on the NIST website:

CAVP Certificate #C1361 (issued on November 16, 2019)

CMVP Certificate #3663 (issued on May 29, 2020)

Cloudian, Inc.
177 Bovet Road, Suite 450 | San Mateo, CA 94402
Tel: 1.650.227.2380 | Email: info@cloudian.com | www.cloudian.com