LYVE™ Cloud

LYVE CLOUD DATA SECURITY

Design, Features, Services

SEAGATE

CONTENTS

Introduction

Seagate® is the industry leader in data-at-rest protection—data security is in our DNA. From consumers walking into a retailer to pick up a backup drive to hyperscale clients purchasing Exos® enterprise-class drives, all our customers trust us with their data. Our proven technology helps to ensure that customers have the highest level of encryption possible, encryption that complies with the strictest government standards. From terabyte-scale drives to the exabyte-scale cloud, Seagate stands for security, delivering on the promise that all customer data will remain customer data.

Building on our history and Seagate Secure™ leadership, data security is a core design tenet of the Lyve cloud exabyte-scale storage as a service. This focus on data security starts with the hardware and extends outward to all aspects of the Lyve Cloud service—including infrastructure, software, features, and process—to align with mature industry standards and benchmarks, as well as third-party certification. Seagate is your secure data custodian—a trusted partner to ensure the confidentiality, integrity, and availability of your data.

SEAGATE SECURE™

The Importance of Security and Data Privacy

The security and privacy of enterprise data is a top priority for our customers. That's because most businesses are subject to industry-specific compliance regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) for healthcare organizations. Similarly, regulations like those of the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) must also be observed.

But compliance isn't the only reason that customers are worried about their data. With cyber attacks becoming increasingly more common, enterprises are looking for protection from malicious ransomware attacks. They're also looking for solutions that will protect their data from accidental deletion and manipulation. As the value of data continues to rise, organizations want assurance that their data remains uncorrupted.

Secure Service – *Maturity in Process and People*

The security and availability of a service's infrastructure and services are only as good as the people and processes that manage the infrastructure and software. Comprised of talented industry veterans, Lyve Cloud has a mature Information Security Management System (ISMS) modeled after IS0 27001. Rigorous controls, strong processes, and comprehensive polices govern the management of Lyve Cloud, resulting in a highly secure, reliable exabyte storage service clearly aligned with the principles of Trust Services Criteria (TSC)—security, availability, process integrity, confidentiality, and privacy.

Lyve Cloud has successfully completed its ISO 27001 and SOC2 certifications. We have a planned roadmap to add on additional certifications based on our customer needs.

Security is an evolving process. We are continuing to take steps toward improving the overall system security and delivering on our promise of trust.

ISO 27001 Controls
Information Security Policies
Organization of Information Security
Human Resource Security
Asset Management
Access Control
Cryptography
Physical and Environmental Security
Operations Security
Communication Security
Systems Acquisition and Maintenance
Supplier Relationships
Security Incident Management
Business Continuity Management
Compliance

Secure Design – *Foundational Security*

The Lyve Cloud service runs on hardened infrastructure that aligns to industry standards such as those set by the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO). During design, the Lyve Cloud team reviewed best practices across leading standards and benchmarks to establish best-in-class hardening guidelines for the entire hardware and software stack.

System and infrastructure deployments are handled through automated configuration management tools to ensure continued compliance with desired state and hardening standards. This capability allows for consistent configurations and security while providing the ability to scale the service rapidly.

Architecturally, the Lyve Cloud service was designed with massive-scale multitenancy in mind from the get-go. Stringent network segmentation and service/process isolation architecture provide multiple layers of security controls. Highly available and resilient infrastructure supports customers' tenant-isolated components, such as the application programming interface (API) gateway, key management, encryption, and the core object storage.

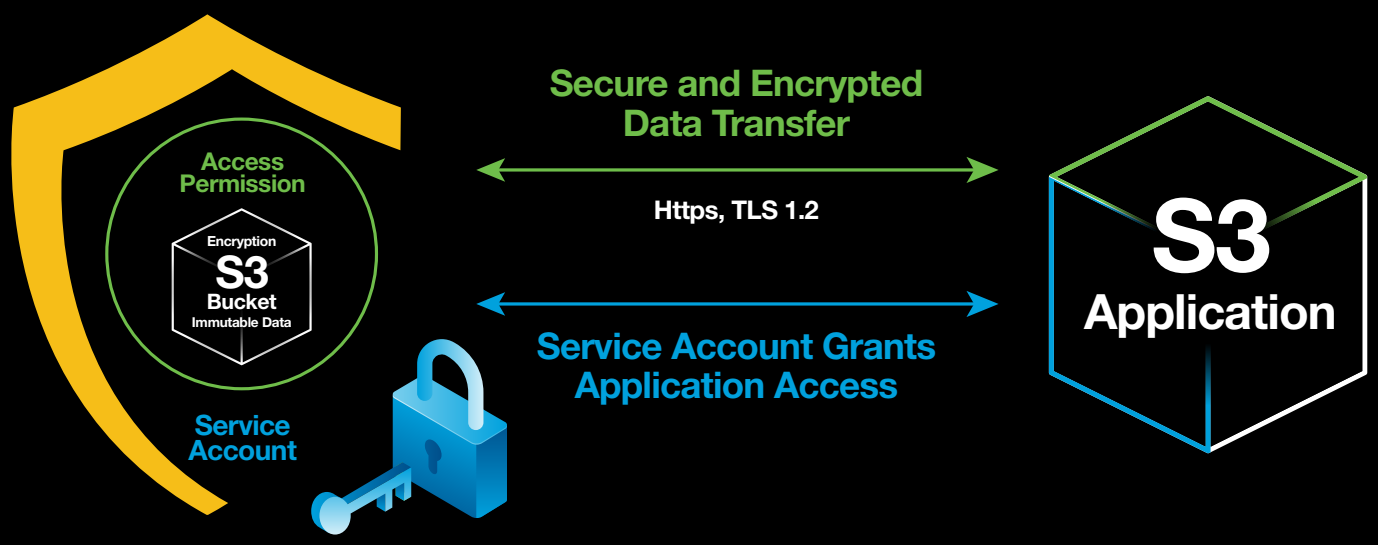
Beginning with the initial design and throughout the duration of testing and implementation, Lyve Cloud partnered with a leading security consulting group. Extensive review of the design and controls were carried out, which culminated in thorough white-box, black-box, and grey-box penetration testing of the service—leaving no stone unturned.

Secure Features – *Secure Data Custodians*

Data security and privacy begins from the moment customers login to the Lyve Cloud portal. This is where users create user accounts and manage their S3 buckets and storage-as-a-service subscription with two-factor identification. When creating an S3 bucket, users can enable compliance mode and object versioning, which will make objects immutable for a fixed amount of time.

To access S3 buckets, customers can create bucket permissions for write- or read-only access. Further, they can create service accounts and select corresponding access permissions. This service account will have its own secret access key, and its credentials will grant access for the application targeting the customer's S3 bucket. Customers can also turn on audit logs per S3 bucket to keep records of their S3 bucket access and usage.

From start to finish, all aspects of the Lyve Cloud portal are user friendly and easily navigable. Customers can rest assured knowing data in flight and at rest is fully encrypted. They can also breathe easy knowing their data integrity is validated to meet compliance and data privacy requirements. Within the Lyve Cloud portal, customers can have clear visibility into Lyve Cloud S3 storage usage. As such, it's imperative that all Lyve Cloud login, user console access, and service account credentials be stored in a safe and secure location.



From the first bits of data transmitted over the wire to the exabytes of data stored on disk, Lyve Cloud's comprehensive data protection assures the confidentiality and integrity of your data throughout its life cycle. This starts with secure communication through transport layer security (TLS), continues through authentication and integrity validation in the API protocol, as well as robust envelope encryption of the object storage with secure key management, and ends with cryptographically secure erasure processes. In this section, we'll dive deeper into these and other security features of the Lyve Cloud service.

Transport Security

The Lyve Cloud service enforces standard TLS 1.2 with 256-bit advanced encryption standard (AES) Galois/Counter Mode (GCM)—otherwise known as AES-256-GCM—to establish secure communications to the customer. As an authenticated encryption algorithm, GCM provides proven security of the symmetric-key cryptographic cipher that has wide adoption for its performance. Seagate storage hardware is validated by Federal Information Processing Standards (FIPS) 140-2/3, which directly aligns with the Lyve Cloud focus on security and performance.

Authentication, Authorization, and Data Integrity

Authentication, authorization, and data integrity are handled in every transaction with the Lyve Cloud API through the authorization header. The authorization header contains both the account's access key and a cryptographic signature. By validating the account access key and verifying the signature—which contains a checksum of the data chunk—the Lyve Cloud API can ensure the validity and integrity of the request before processing it further.

Secure Data In-Transit

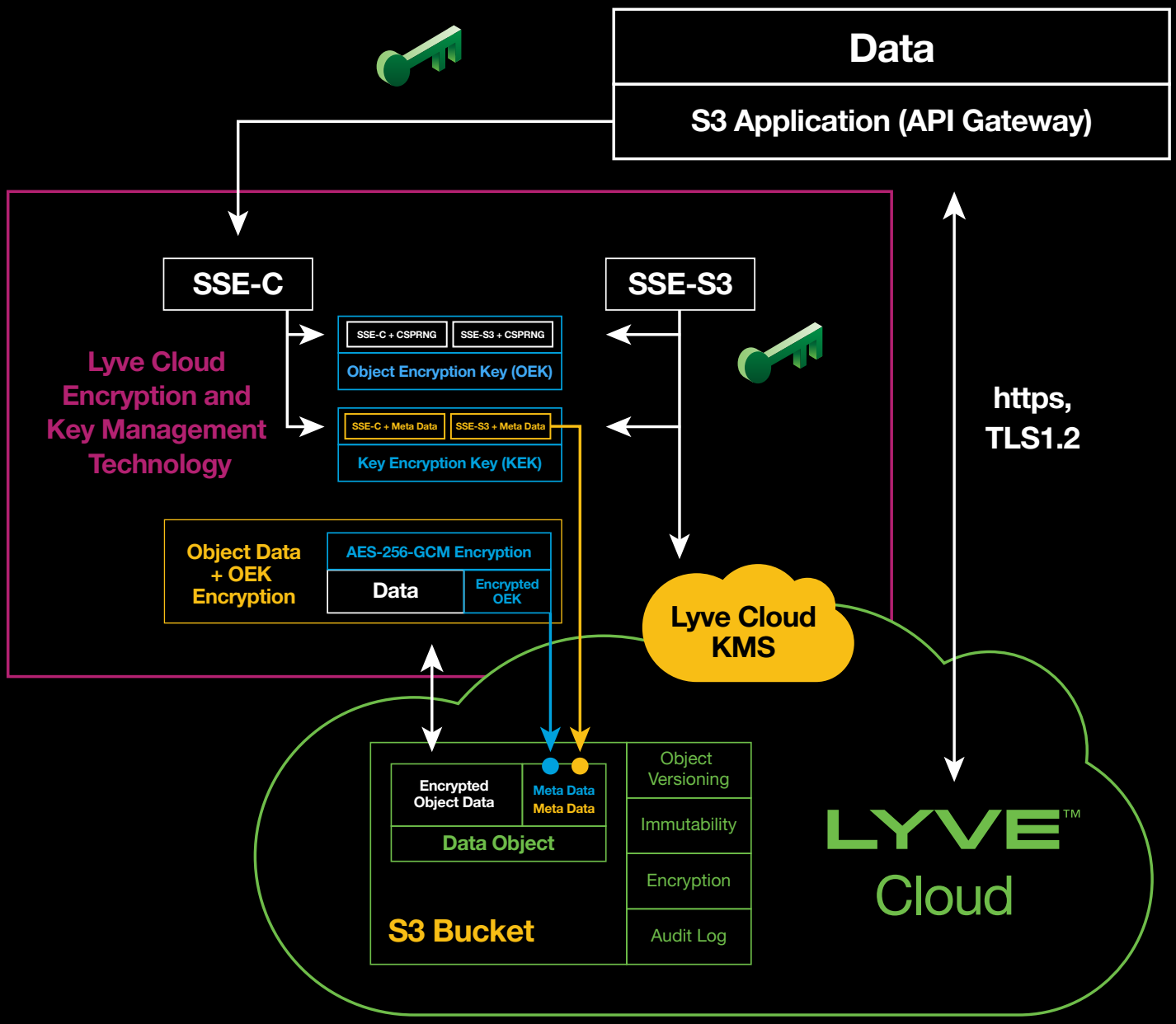
Envelope Encryption and Key Management

A key security feature of Lyve Cloud is that all data is encrypted before it's stored, regardless of whether it's encrypted at the source. There is no option to dial back the protection. Two options for server-side encryption are supported:

- Server-Side Encryption with Client-provided key (SSE-C)
- Server-Side Encryption with a key generated by the Lyve Cloud Key Management System (KMS) (SSE-S3)

In both SSE-C and SSE-S3, the key used for object encryption—the Object Encryption Key (OEK)—is uniquely generated using a Cryptographically Secure Pseudo-Random Number Generator (CSPRNG). The OEK is never stored in clear text; rather, it's stored in encrypted form as part of the object metadata. The OEK is encrypted by the Key Encrypting Key (KEK), which is generated by a key-derivation algorithm using either the client-provided key (SSE-C) or Lyve Cloud KMS key (SSE-S3) and other object-specific metadata. The cryptographic primitive used for all the object encryption operations is AES-256-GCM.

Data Encryption and Key Processes



Secure Erase

Lyve Cloud's envelope encryption, which uses strong AES-256-GCM, requires that either a client key (SSE-C) or the client's unique master key from the Lyve Cloud KMS (SSE-S3) is provided to derive the KEK that is used to encrypt the OEK that's stored in the metadata of the object. Without this access to the KEK, the data object is cryptographically secure. Cryptographic erasure, leveraging FIPS 140-2/3-validated encryption algorithms, is recognized by NIST 800-88 and ISO/IES 27040:2015 as a suitable—and even preferred—method of data/media sanitation.

When a customer chooses to end their tenancy with Lyve Cloud, they can be confident that their data will be securely cryptographically erased in compliance with recognized FIPS/NIST/ISO standards. With client-provided keys (SSE-C), the key that's used to derive the KEK is only provided by the customer in the API request. Since this is never stored by Lyve Cloud, customers using SSE-C render the object data cryptographically erased by deleting or simply not using the key. In the case of SSE-S3, where the client's unique Customer-Managed Key (CMK) is generated by the Lyve Cloud KMS, which is managed in a secure enclave, the CMK account is deleted upon tenant termination, effectively destroying the customer unique keys necessary to deriving the KEK.

Conclusion

Lyve Cloud was crafted with data security and privacy in mind. With hardened infrastructure that aligns to guidelines set by NIST and ISO, our storage-only cloud meets the most stringent global security standards. This is further demonstrated by our ISO 27001 and SOC-2 certifications.

Lyve Cloud is hosted in Tier 4 data centers, ensuring the highest class of data center availability and access. By design, data encryption cannot be disabled within Lyve Cloud. This means data is always encrypted at rest and in flight. Further, ransomware protection safeguards data from malicious attacks while object immutability protects data from accidental manipulation or deletion.

Seagate believes that customer data belongs to the customer. Therefore, Seagate will never use or access any data stored in a Lyve Cloud S3 repository. With zero backdoors and high-level security features, Lyve Cloud puts the customer in full control of their data.

Ready to Learn More?

Visit us at seagate.com/services/cloud/storage
Or download the brochure

seagate.com

TP730.1-2105US May 2021

SEAGATE