Object Lock

Immutable cloud object storage for ransomware resilience, compliance retention, and chain-of-custody protection

Object Lock is a data protection capability that prevents protected object versions from being modified, overwritten, or deleted during a configured retention period. In practical terms, it helps organizations preserve critical backups, archives, records, logs, surveillance video, and other evidence-grade data in a Write Once/Read Many (WORM) state. That means it is written once and cannot be altered or deleted, but can be read many times.

For cyber-resilience, Object Lock should be part of a layered architecture. Immutable data is harder to destroy, but the surrounding account, bucket, identity, and administrative controls must also be hardened. Wasabi combines Object Lock with controls such as Multi-Factor Authentication (MFA), Identity Access Management (IAM) policies, logging, encryption, legal hold workflows, and Multi-User Authorization for selected sensitive account activities.

Object Lock benefits

- Object-version-level retention control
- Governance and compliance retention modes
- Legal hold support for selected object versions
- Protection against overwrite and deletion during retention
- Ransomware and administrator-error risk reduction
- Support for retention and chain-of-custody workflows

Layered security add-ons

- MFA for privileged users
- Multi-User Authorization for specified sensitive or destructive activities
- Least-privilege IAM policies and separate admin roles
- Encryption and secure transport configuration
- Administrative and compliance logging
- Replication and account separation for blast-radius reduction

Challenges with protecting data

Many organizations still associate true protection with offline or air-gapped media. Physical air gaps can reduce online attack paths, but they also slow recovery, add handling and media-management overhead, and can complicate routine validation. Ransomware operations increasingly target backup and archive environments because recovery copies determine whether the victim can restore without paying.

Object Lock helps close that gap by making protected object versions non-erasable and non-overwritable for the defined retention period while keeping the data available in hot cloud storage. This safeguard supports rapid recovery, legal review, audit response, and evidence preservation without reverting to slow retrieval workflows.

Why Object Lock matters

- Staff changes: Staff turnover, permission drift, and administrative mistakes can put retained data at risk.
- Attackers target recovery: Ransomware campaigns often attempt to delete, encrypt, or corrupt backup copies before launching the primary extortion event.
- Regulators and auditors care about retention: Records, logs, and transactional data may need provable preservation.
- Evidence integrity matters: Surveillance video, digital evidence, and investigation data need chain-of-custody controls in an era of manipulated media.
- Recovery confidence depends on operational proof: Immutable copies should be tested, logged, and mapped to restore runbooks.

Compliance Mode and Governance Mode

Wasabi Object Lock supports two retention modes: Compliance and Governance. Compliance mode is the stricter setting: protected object versions remain immutable until the retention period ends, and the retention date cannot be shortened.

Governance mode allows authorized users with special permissions to adjust or bypass retention controls when business policy permits.

Both modes can support legal hold workflows for object versions. A legal hold is useful when a retention requirement extends beyond a normal retention schedule, such as during litigation, an investigation, an audit, or evidence preservation.

Mode selection guidance

- Use Compliance mode when data must not be deleted or altered before the retention period expires.
- Use Governance mode where privileged, policy-approved administrators may need controlled override capability.
- Use legal hold when a specific object version needs protection independent of the normal retention date.
- Do not use immutability as a substitute for identity controls, access review, logging, and restore testing.

Object Lock vs. bucket-level compliance

Wasabi provides two approaches to immutability: Object Lock and bucket-level compliance. These are mutually exclusive on a bucket. A bucket can use either Object Lock or bucket-level compliance, but not both. Because Object Lock must be enabled before use and is commonly selected at bucket creation, teams should decide the retention architecture before placing production data in the bucket.

Object Lock is the better fit when teams need object-version-level retention, legal hold workflows, or application-driven retention policies. Bucket-level compliance is a strong fit when teams need WORM-style immutability for the contents of a bucket, enforced by a defined policy.

- Use Object Lock for granular object retention, legal holds, backup application integration, and evidence-grade retention workflows.
- Use bucket-level compliance for broad WORM-style protection where objects should follow a uniform bucket policy.
- Document the retention owner, retention period, exception process, and recovery test cadence before go-live.

Add Multi-User Authorization to protect the control plane

Object Lock protects object versions, but the control plane around those objects also needs protection. Multi-User Authorization adds a second-person approval layer for specified sensitive activities. A root user can add up to three security contacts, who must all sign off on specified account activities. MFA must be enabled before security contacts can be added.

This protection is directly relevant for buckets and accounts that contain immutable data. If a destructive action, such as account or bucket deletion, requires additional approval, a compromised administrator credential is less likely to become a single point of catastrophic failure. Multi-User Authorization complements Object Lock by protecting the environment that contains the immutable recovery copies.

Recommended security pattern for immutable buckets

- Enable MFA before assigning privileged roles or security contacts.
- Configure Multi-User Authorization for destructive account or bucket activities where available.
- Separate the backup operator, storage administrator, and security approver roles.
- Avoid using root credentials for routine backup operations.
- Use least-privilege access keys scoped to the backup workflow.
- Monitor administrative activity and test deletion-denial scenarios as part of resilience exercises.

Lock out data loss with Wasabi

Protect the recovery copy and the controls around it. Use Wasabi Object Lock or bucket-level compliance for immutable data retention, pair it with MFA and least-privilege IAM, and add Multi-User Authorization for sensitive destructive actions in backup and archive environments.

About Wasabi

Wasabi provides simple, predictable, and affordable cloud object storage for organizations that need to store, protect, and instantly access growing volumes of data. With S3 compatibility, hot storage access, strong security controls, and predictable pricing, Wasabi helps organizations modernize backup, archive, media, surveillance, AI data pipelines, and long-term retention use cases.