wasabi®
hot cloud storage

What is Covert Copy?

Simple, predictable, and affordable cloud storage fit for storing the world's data

Our newest feature aims to prevent and minimize the impact of ransomware attacks by providing logically air-gapped cloud object storage that goes one step further than immutability alone. Covert Copy replicates a bucket, significantly limits access, and makes it immutable and indestructible.

Covert Copy enables Wasabi admins with root access to create a hidden, inaccessible, and tamper-proof copy of their data. Only the root user, using our Multi-User Authentication (MUA) feature, can make the data accessible when absolutely necessary.

Benefits:

› In-depth data protection that is simple to implement

› Combat ransomware

› Avoid accidental data erasure

› Ensure regulatory compliance

Challenges of ransomware and data protection

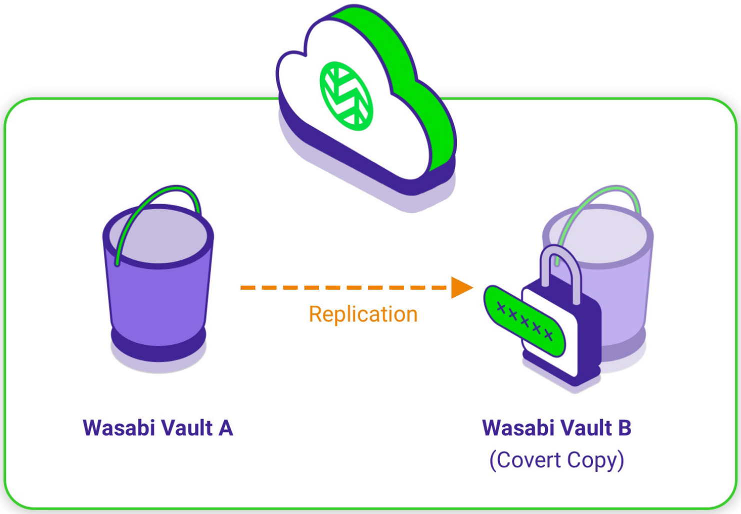
Cyber criminals are leveraging AI to target both customers and partners, disrupting entire supply chains. A key part of any ransomware attack is stealing business-critical, sensitive data, then encrypting or destroying that same data. Backup data has become part of the attack method to increase damage and demand the highest possible ransom.

Our innovative solution allows you to create a duplicate of your data in a secure, covert bucket. This means it is invisible to any non-root users and can be made immutable for a specified retention period that automatically renews. A Covert Copy bucket can only be accessed through a dual-authenticated user via MUA.

How Covert Copy works

Covert Copy is restricted to use by the root user and is managed through the Wasabi console. A root user creates a Covert Copy bucket by first choosing a source bucket from their Wasabi Hot Cloud Storage. The data from the source bucket is then copied to a new Covert Copy bucket, which remains invisible to non-root users, becomes immutable through object lock, and is inaccessible unless the root user and authorized users grant permission via Multi-User Authentication (MUA).

- Managed using the Wasabi Console
- Limited to use by root user
- Requires use of Multi-Factor Authentication (MFA)
- Requires use of Multi-User Authentication (MUA)
- Replicates all or filtered contents of the source bucket
- Leverages Wasabi Object Lock for immutability (object integrity)
- Renews lock every 30 days automatically
- Practically "untouchable" and "impenetrable"



Use Cases for Covert Copy

Covert Copy is an ideal solution for ransomware protection. Use Covert Copy for any use cases where you need an extra layer of protection for sensitive data:

Backup data – Create a secure, invisible, and immutable copy of backup data that can't be found by a non-root user. More than just ransomware mitigation, Covert Copy prevents a ransomware attack by making the data in a Covert Copy bucket unfindable and inaccessible.

Archiving and compliance – Create a Covert Copy of a subset of archived content that is particularly sensitive (e.g.: AI data sets, Intellectual property such as patent info, personally identifiable Information (PII), medical records, etc.) or other data subject to compliance mandates.

Golden copy for disaster recovery – Root user can create a pristine copy of critical buckets that can only be accessed through a gated approval process.

Wasabi Covert Copy is included with Wasabi Hot Cloud Storage and delivers enterprise-grade, virtually air-gapped storage that is easy to configure and operate. Our cyber-resilient storage solution not only reduces the impact of ransomware attacks but also prevents them.

Wasabi Partners: Position Covert Copy as a built-in security enhancement to Wasabi Hot Cloud Storage during ransomware, backup, and compliance discussions. Use this brief to highlight the added value of protection beyond immutability and to help customers identify data sets that would benefit from an additional, covert layer of immutable protection.

Customers: Work with your Wasabi partner to understand how Covert Copy can be enabled for your organization. Adding a hidden, tamper-proof copy of critical data can enhance ransomware resilience and support confident recovery.