

Object First + Veeam Data Cloud Vault = 3 2 1 Backup

What is 3-2-1, and Why Does it Matter?

The [3-2-1 backup](#) rule has long been the foundation of backup methodology and data protection through redundancy, resilience, and dispersion. It guarantees that a company's information can be recovered in the event of disaster, whether due to a cyberattack, hardware failure, natural disaster, or insider threat.

Specifically, the rule stipulates that organizations should maintain:

- **Three copies of data:** Including the original data and two redundant copies, reducing the risk of data loss due to corruption or accidental deletion.
- **Two different media types:** Such as tape, cloud storage, external hard drives, or network-attached storage (NAS), which mitigates the potential for media-specific failures.
- **One copy stored offsite:** To protect against natural disasters like floods, fires, or other catastrophic events that could compromise all onsite data.

Implementing the 3-2-1 backup rule ensures data durability, enhances recovery capabilities, and strengthens overall business resilience against everyday operational risks and exceptional catastrophes.

Although it's [now an IT industry standard](#), the rule has roots in photography.

Conceptualized by photographer Peter Krogh in 2005, the 3-2-1 backup rule first debuted in his book *Digital Asset Management for Photographers*.



Peter Krogh.
American photographer
Courtesy of The [DAM Book](#).

Why 3-2-1 Is Key to Ransomware Resilience

The 3-2-1 backup policy is the only way to ensure ransomware resilience for backups because it emphasizes the importance of maintaining at least one copy of data that is offline, air-gapped, or immutable—conditions needed for defending against malicious encryption and mass data corruption typical of ransomware attacks.

Ransomware often targets connected, accessible backups, rendering them useless. Storing one backup copy in an immutable, offline state—like on WORM media or in an air-gapped environment—reduces this risk. This single, resilient copy acts as a fail-safe, ensures clean data recovery, thereby ensuring business continuity and minimizing ransomware damage.

The Extra 1 and 0: Immutability & Verification

The [3-2-1-1-0](#) backup rule further expands on the traditional 3-2-1 model, bolstering ransomware resilience by incorporating additional safeguards. The extra “1” refers to keeping at least one extra copy in an immutable or air-gapped state, ensuring that even if attackers gain access to primary backup systems, they cannot modify or delete this protected copy. The “0” represents zero errors upon backups, ensuring that all backup copies are free from corruption, malware, or configuration errors.

Finding the Right Backup Solution

Admins should choose solutions that enable integration across on-premises and cloud environments, facilitate frequent testing to ensure backup integrity, and, most importantly, support immutable and air-gapped backups.

Securing the On-Prem Copy

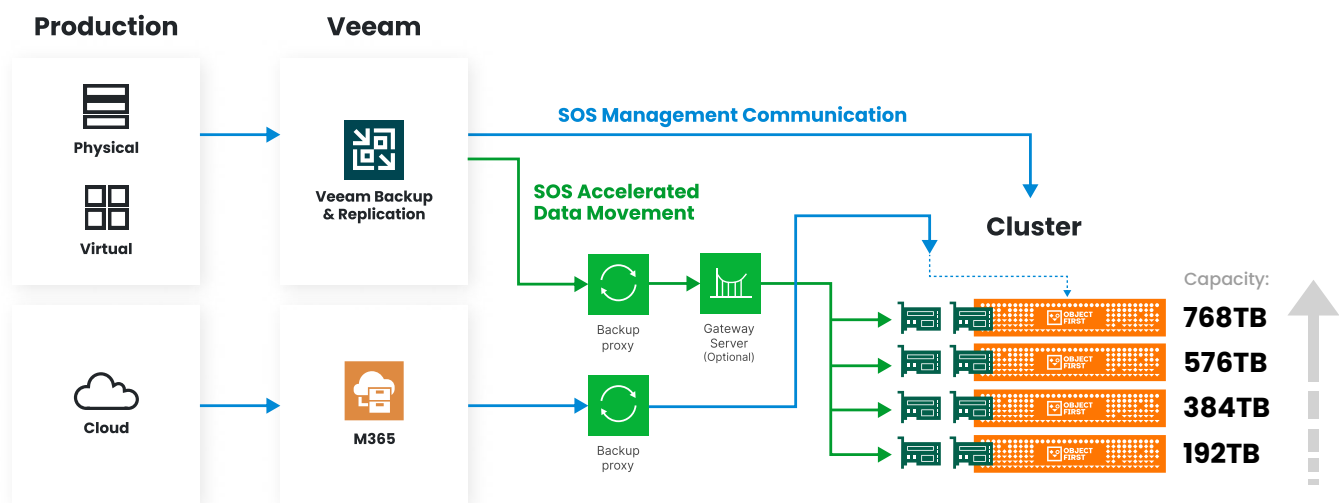
[Object First's Ootbi \(Out-of-the-Box Immutability\)](#) is the best storage for Veeam on-premises backup data, aligning perfectly with the principles of the [3-2-1-1-0 backup rule](#) by providing security, simplicity, and power. In this framework, having at least two copies in different locations is crucial—one for fast, local recovery and another off-site for protection against large-scale disasters like cyberattacks or physical damage.

On-premises storage plays a unique role by offering the fastest recovery path, ensuring data remains readily accessible when needed. Unlike cloud vaults, which may face bandwidth constraints, on-premises appliances enable rapid restore operations without reliance on external connectivity.

Ootbi—Ransomware-proof Backup Storage

Ransomware-proof and immutable out-of-the-box, Ootbi is Secure by Design as defined by CISA. Ootbi was built around the latest Zero Trust principles, which follow an “Assume Breach” mindset that accepts individuals, devices, and services attempting to access company resources as compromised and should not be trusted. Ootbi utilizes S3 Object Lock to enable immutability and runs on a hardened Linux operating system with zero access to perform destructive actions to the firmware, operating system, storage layer, or backup data.

Object First and Veeam Backup & Replication Architecture



Ootbi’s inherent separation from the Veeam Data Platform creates a clear boundary, isolating backup data from other system components. As a result, it reduces the likelihood of ransomware or other attacks spreading from the main platform to the backup storage. The dedicated hardware also facilitates independent updates and hardware redundancy, which helps protect data and enhance recovery reliability. This physical segmentation is a vital aspect of safeguarding backup data and ensuring quick, secure recovery during a cyberattack. In fact, it’s the only thing that enabled an [Object First customer in an Ohio school district](#) to recover their data without damage during a cyberattack.

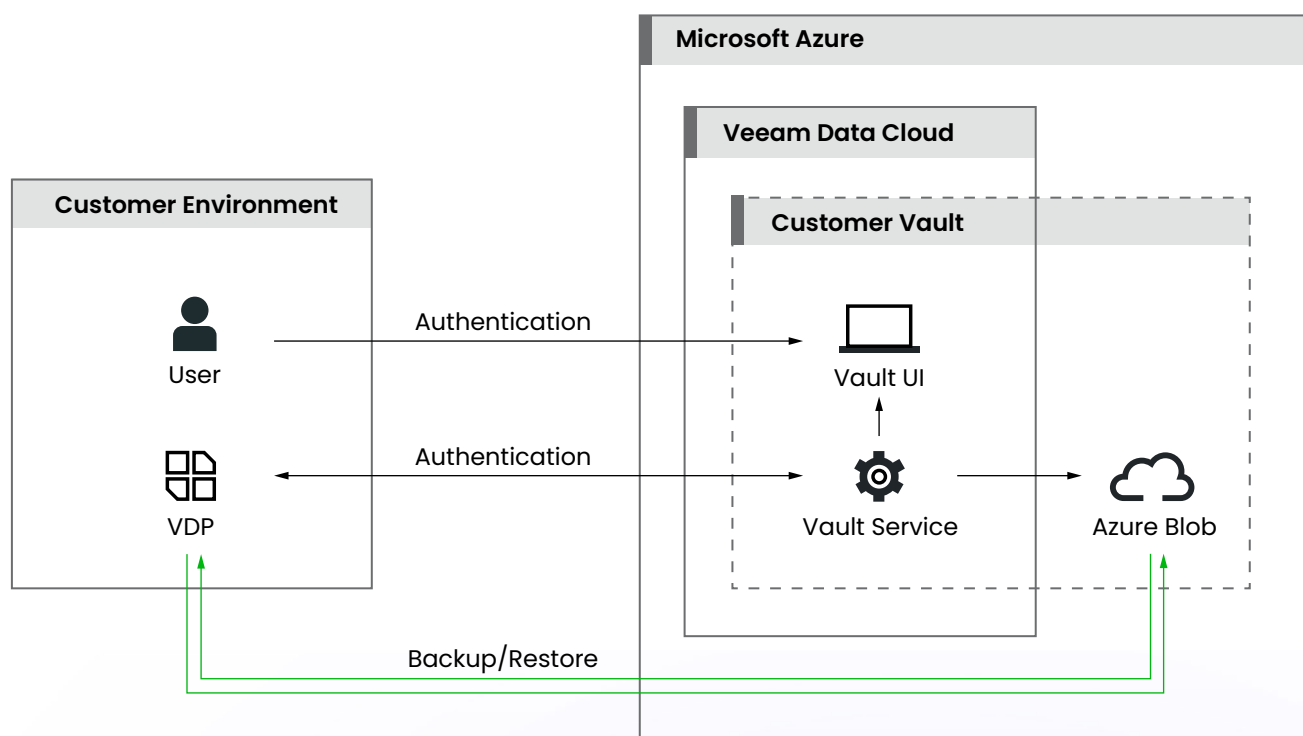
Ootbi is a 2U backup storage appliance that reduces management complexity with built-in hardware redundancy and automatic updates for firmware, OS, and software. It takes less than 15 minutes to configure, requires zero security expertise to manage, and does not require additional setup or namespace adjustment at the Veeam layer when scaled. Ootbi was purpose-built for the Veeam environment and is the best option for a primary storage target for local backup data.

Choosing the Off-Site Storage

[The Veeam Data Cloud Vault](#) offers a secure, easy, and predictable off-site storage solution that meets modern data protection needs. One of its editions, the [Veeam Foundation Model](#), establishes a standardized approach to backup security, immutability, and resilience, ensuring optimal data protection. As a fully managed, pre-configured cloud storage service on Azure, it eliminates the complexities of infrastructure management and unpredictable costs, allowing organizations to focus on their core operations.

The service provides Zero Trust security out-of-the-box, ensuring that backup data remains immutable and logically air-gapped from the production environment. With predictable, all-inclusive pricing based on a flat per-TB rate, Veeam Data Cloud Vault simplifies budgeting and capacity planning, making it easy to scale as your needs grow.

Veeam Data Cloud Vault Architecture



Veeam Data Cloud Vault is currently supported by the Veeam Data Platform and Kubernetes backups by Kasten only.

Simple Secure Cloud Storage

Ideal for organizations seeking resilient and secure backup storage, Veeam Data Cloud Vault creates multiple copies of data across datacenter or regions, offering high levels of data durability—11 nines (99.999999999%) or 12 nines (99.9999999999%), depending on the offering—all while maintaining encrypted and immutable data states. As part of Veeam Data Cloud Vault, the Foundation Model prioritizes a secondary local copy to reduce reliance on cloud retrieval, ensuring faster recoveries without excessive egress costs.

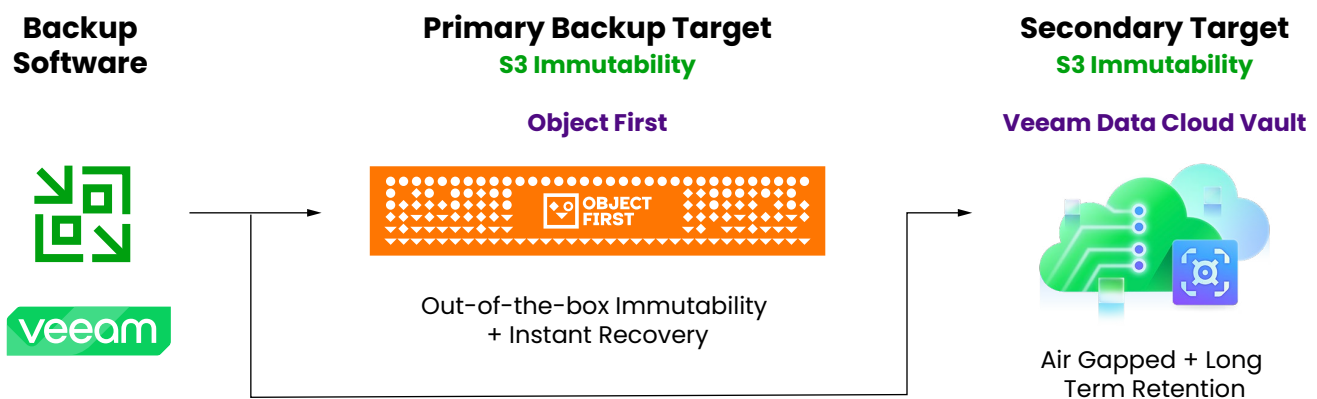
Designed for high availability, the service ensures protection against outages and failures with durable, synchronous replication, offering confidence that backup data remains accessible for rapid recovery when needed. This approach follows Veeam's principles of optimizing backup structures to prevent unnecessary cloud fetches, reinforcing business continuity with local-first recovery strategies. Whether serving as a primary or secondary off-site storage solution, Veeam Data Cloud Vault delivers the flexibility, security, and predictability necessary to mitigate cyber threats of all sizes.



Ensure Ransomware Recovery with a Tested 3-2-1-1-0 Solution

When paired with Object First's Ootbi, Veeam Data Cloud Vault solution provides an ironclad approach to data protection that fulfills the criteria of the 3-2-1-1-0 backup policy. Ootbi ensures ransomware resilience with purpose-built on-prem immutable storage, while the Veeam Data Cloud Vault offers secure, managed off-site storage that simplifies scalability and cost management.

Acting as a second layer of defense, the vault ensures that even if primary backup environments are unavailable, recovery remains intact. Its immutable design and logical air-gapping make unauthorized access and ransomware encryption attempts impossible, preserving critical data integrity. Together, these solutions establish a powerful solution that not only meets industry best practices but also proactively defends against sophisticated cyberattacks.



Predictable Pricing, Your Way

Complementing Veeam Data Cloud Vault's all-inclusive pricing, Object First offers a pay-per-use Consumption model—delivering immutable backup storage without upfront investments or hardware lifecycle costs. Customers can scale from 17 TB to 7 PB with simple monthly billing and a 1-year subscription, ensuring cost efficiency and predictable management.

Discover how Object First and Veeam Data Cloud Vault can strengthen your data resilience—[request a demo today](#) to see their joint capabilities in action!

objectfirst.com

© 2025 Object First. All rights reserved. All trademarks are the property of their respective owners.

