3 Reasons Ootbi* is Best Storage for Veeam

* Out-of-the-box immutability

## Veeam customers need secure, simple, and powerful storage

Veeam customers are refreshing their current on-prem backup storage and looking for a secure, simple, and powerful, ransomware-proof solution that won't break the budget and provides fast backup and Instant Recovery.

Admins are limited by legacy solutions like DAS (Direct-Attached Storage), dedupe appliances, or Hardened Linux Repositories that are not explicitly optimized for Veeam. They require security expertise and expensive technical staff to manage and compromise security, simplicity, or power.

Finding the proper storage solution starts with understanding what current solutions lack.

Radar chart with axes Secure, Simple, Powerful comparing Veeam Customer Needs and Legacy Solutions.
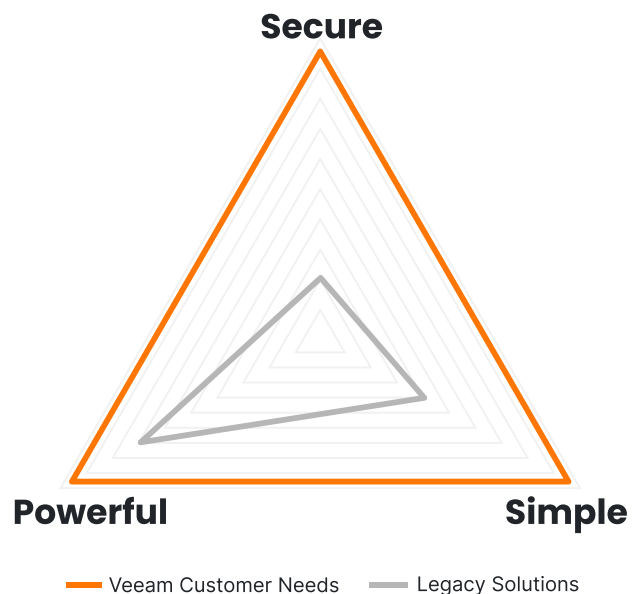
Veeam Customer Options for On-Prem Storage
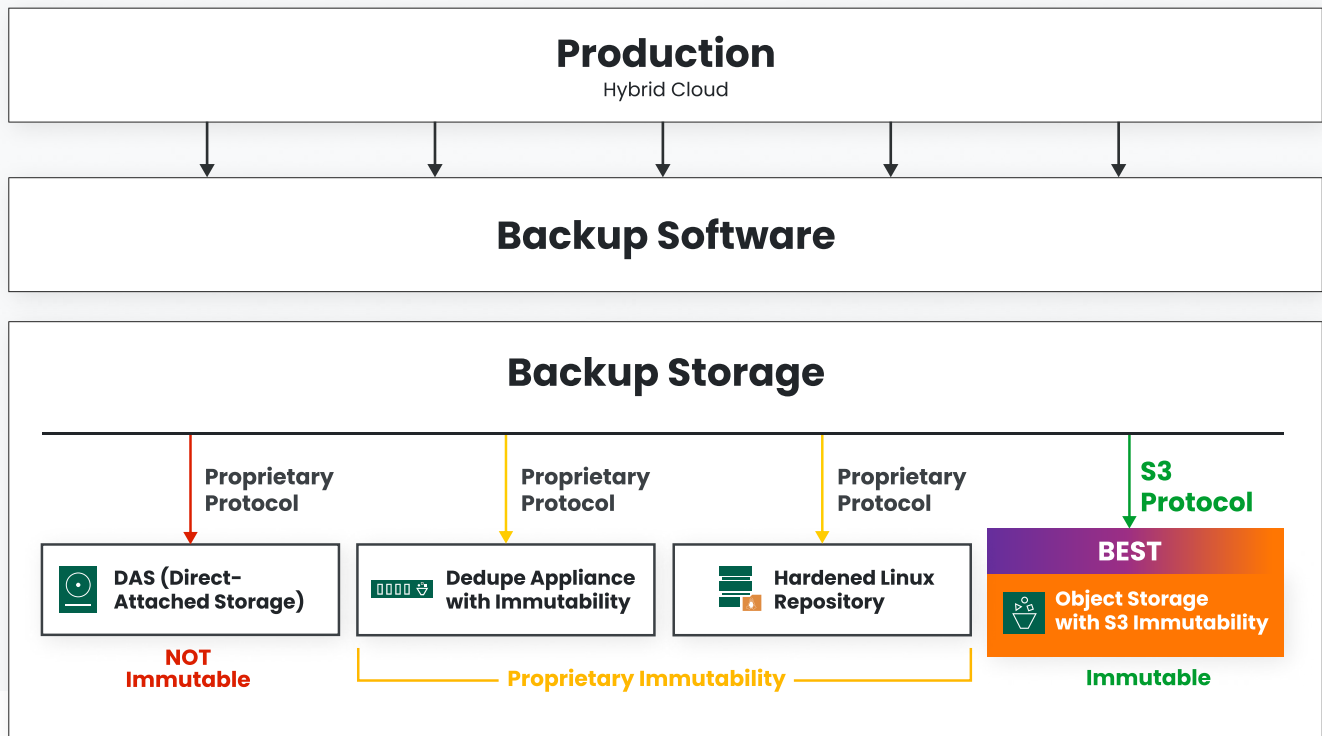
Direct Attached Storage

Direct Attached Storage (DAS), which delivers file and block storage, has been the standard for decades. It can be as powerful as the hardware it runs on and requires very little training or experience to implement due to its familiarity. But this comes at the cost of weak security. Because DAS does not offer immutability and is attached directly to the Veeam Backup & Replication server with no separation of Backup Software and Backup Storage, an attacker who gains access to the host by exploiting an OS or application vulnerability can access all data on that system. DAS is no longer suitable to be a backup storage target because of these security weaknesses (see Figure 2).

Deduplication Appliances

Dedupe appliances make an excellent long-term retention target as a Capacity or Archive Tier for Veeam. Still, every admin knows the hit in performance resulting in very slow Veeam Instant Recovery due to rehydration on restore. Deduplication appliances make data encryption choices complex and may expose and compromise raw Veeam backup data in the event of a breach. They suffer either from requiring expertise in the product or demanding a white-glove installation to get the most out of the storage, not to mention that security is often an add-on with no simple options for out-of-the-box Veeam integrated immutability. They do not meet modern security demands and should never be chosen as the first choice for recovery when a ransomware event occurs.

Hardened Linux Repositories

The Hardened Linux Repository (HLR) is one of the more recent additions to the Veeam admin's storage options, and it excels at being secure, so long as you have domain expertise in security and Linux and time to keep it up-to-date. HLRs are by far the best choice of the three options examined. However, the amount of work required to set them up, keep them secure and updated, and perform to expectation is not feasible for most Veeam admins in the mid-enterprise to take on in addition to their day-to-day responsibilities.

	Direct Attached Storage	Deduplication Appliances	Hardened Linux Repositories
Secure	❌ **No.** It does not offer immutability and is located in the same operating environment as the backup software, with no separation of Backup Software and Backup Storage.	❓ **Variable.** Immutability is an afterthought, not integrated with Veeam's workflow. It requires manual configuration and security expertise and makes data encryption choices complex.	❓ **Variable.** It varies based on the user's security and Linux expertise. It also requires a significant amount of time and willingness to keep Linux updated.
Simple	✅ **Yes.** Due to its legacy, all technical professionals understand how to utilize this fundamental storage.	❌ **No.** Requires either a white-glove service or training to configure. Expertise in both storage and security is necessary to maintain.	❌ **No.** Expertise in security and Linux is required to configure and maintain. Dedication and vigilance for updates and responding to zero-day exploits are mandatory.
Powerful	❓ **Variable.** It can be as powerful as the hardware it runs on.	❌ **No.** Great for archiving large volumes of data and long retention periods. Veeam Instant Recovery is especially slow due to the time required to rehydrate the deduplicated data.	❓ **Variable.** It can be as powerful as the hardware it runs on.

None of these options fulfills the Veeam admin's need for a simultaneously secure, simple, and powerful solution.

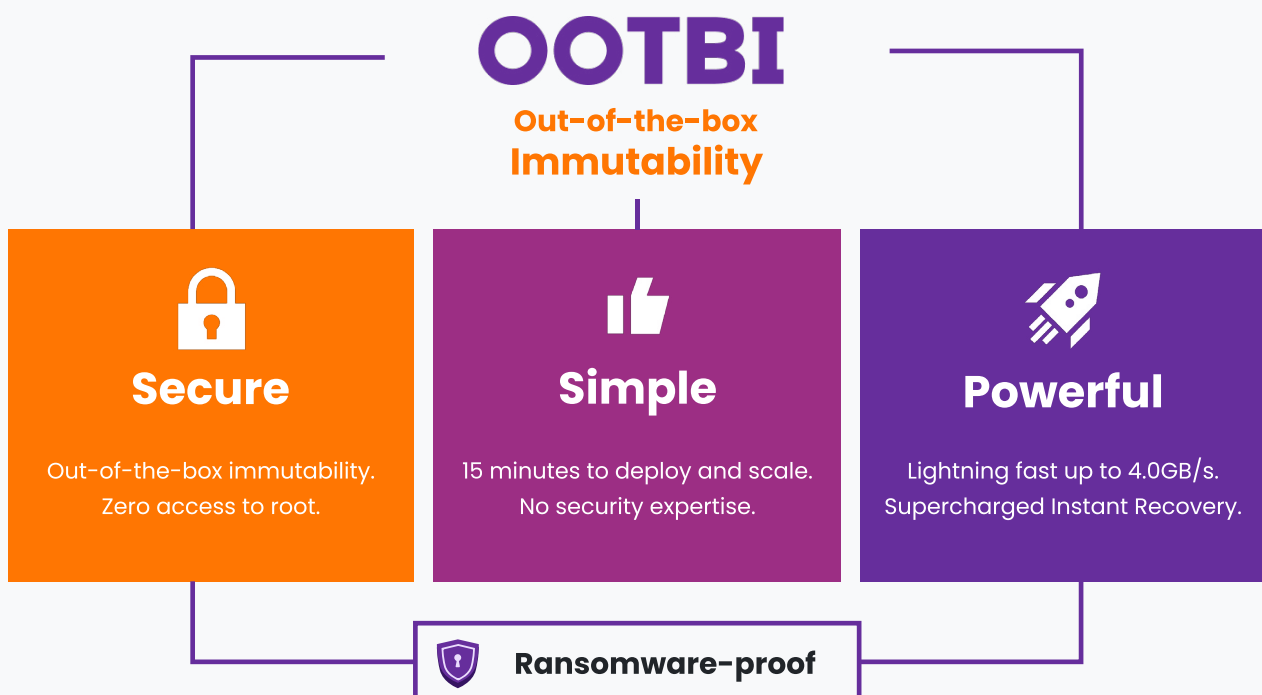### They need the Best Storage for Veeam.

OOTBI* —
Best Storage for Veeam

* Out-of-the-box immutability

Today, businesses need a purpose-built, ransomware-proof, on-prem storage target that integrates seamlessly with Veeam and guarantees the security of its backups. Ootbi, which stands for out-of-the-box immutability, is secure, simple, and powerful by design and delivers a ransomware-proof primary storage target that was purpose-built to be the best storage for Veeam.

Veeam Data Platform V12 fully embraces S3 Object Storage as a primary backup target. Ootbi fully supports Veeam's "direct-to-object" functionality leveraging industry-standard S3 object storage security and immutability while providing high-performance backup. It also fully supports Veeam Smart Object Storage API (SOSAPI) for simplified management.

Best Storage for Veeam

OOTBI
Out-of-the-box Immutability

Secure

Out-of-the-box immutability. Zero access to root.

Simple

15 minutes to deploy and scale. No security expertise.

Powerful

Lightning fast up to 4.0GB/s. Supercharged Instant Recovery.

Ransomware-proof

Zero Trust Data Resilience (ZTDR)

Zero Trust, Zero Trust Architecture, and the Zero Trust Maturity Model are modern IT security paradigms developed and endorsed by numerous security organizations, including CISA and NIST. At its core, Zero Trust replaces the "perimeter security" approach, which is no longer effective in hybrid cloud, mobile, and remote work. The Zero Trust framework is being adopted as the new IT security standard by the US government and mid- and large enterprises worldwide, especially in data-sensitive industries like banking, healthcare, technology, manufacturing, and others.

Backup infrastructure inherently has a large attack surface, as it requires read and write access to production systems. Zero Trust requires that the backup infrastructure be segmented into multiple security domains or resilience zones, such as Backup Software, Primary Backup Storage, and Secondary Backup Storage — each with its own reduced attack surface. In this case, the Backup Software may still have an exposed attack surface, but the Backup Storage will have a minimal attack surface. This is achieved by limiting communication to an industry-standard S3 protocol (See Figure 1).

Security and data protection experts Numberline Security and Veeam have proposed Zero Trust Data Resilience (ZTDR), explicitly extending Zero Trust principles to Backup and Recovery infrastructure. More information is available at: Zero Trust Data Resilience: Secure Backup and Recovery Architecture — A Pragmatic Approach to Zero Trust by Veeam.

Following ZTDR principles Object First recommends ensuring your backup storage security by implementing the following:

- Segmentation — separation of Backup Software and Backup Storage.

- Multiple data security domains or resilience zones to ensure multi-layered security.

- S3-native object storage immutability.

- S3-native security, least-privilege access, IAM and MFA.

- S3 communication protocol with minimal attack surface for Backup Storage.

- Zero access to root and OS, protecting against malicious or compromised administrators.

- Open design and architecture, simplifying enterprise adoption and deployment.

3 Reasons Ootbi is Best for Veeam

1. The Best Storage is Secure

Ootbi was built to support Zero Trust principles — including Veeam's recommended Zero Trust Data Resilience (ZTDR) architecture (See Figure 1), which assumes that individuals, devices, and services attempting to access company resources are compromised and should not be trusted. Ootbi follows Cybersecurity and Infrastructure Security Agency (CISA) recommendations* and embodies the principles of "Security-by-Design and -Default." Ootbi utilizes S3 Object Lock to enable immutability and runs its storage software on a hardened Linux operating system with a "zero access to root" policy. Due to the ZTDR architecture and secure appliance form factor, Ootbi is inherently separated from the Veeam Backup & Replication server, unlike legacy solutions such as DAS (See Figure 2), creating the proper segmentation between Backup Software and Backup Storage layers to ensure ransomware resilience.

Figure 1

Zero Trust Data Resilience (ZTDR) architecture

**Separation of Backup Software and Backup Storage**
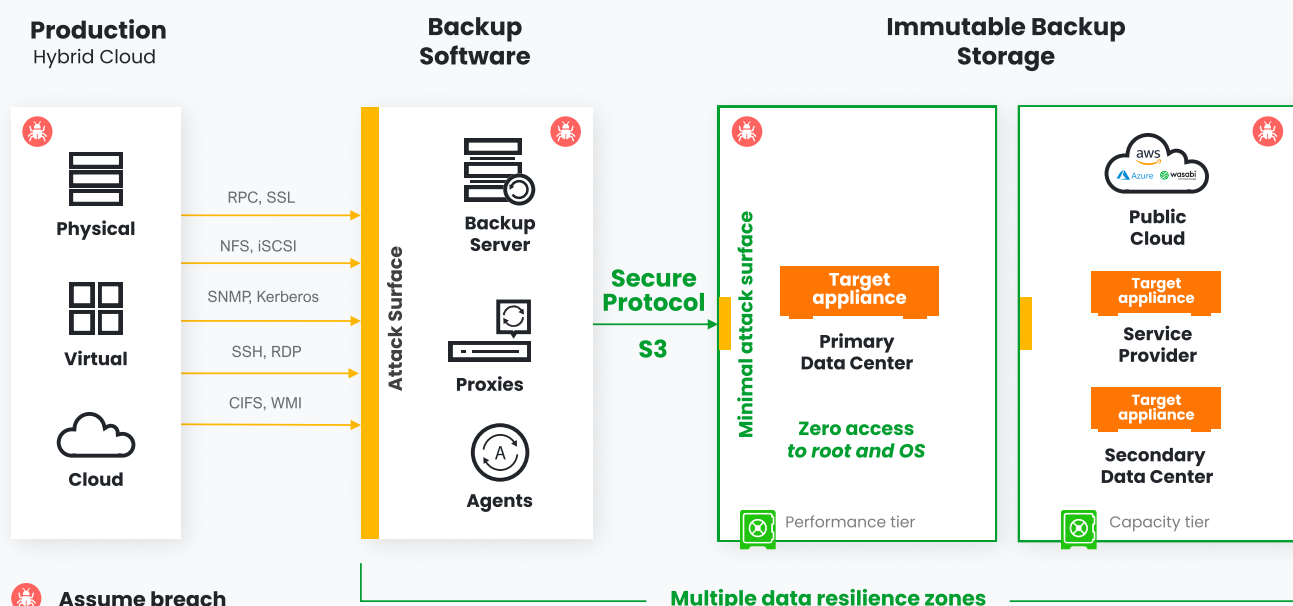
*Cybersecurity and Infrastructure Security Agency. (2023). Shifting the balance of cybersecurity risk: Principles and approaches for security-by-design and -default. Retrieved from https://www.cisa.gov/sites/default/files/2023-04/principles_approaches_for_security-by-design-default_508_0.pdf

Figure 2

DAS — Direct-Attached Storage

NOT Zero Trust. No separation of Backup Software and Backup Storage.
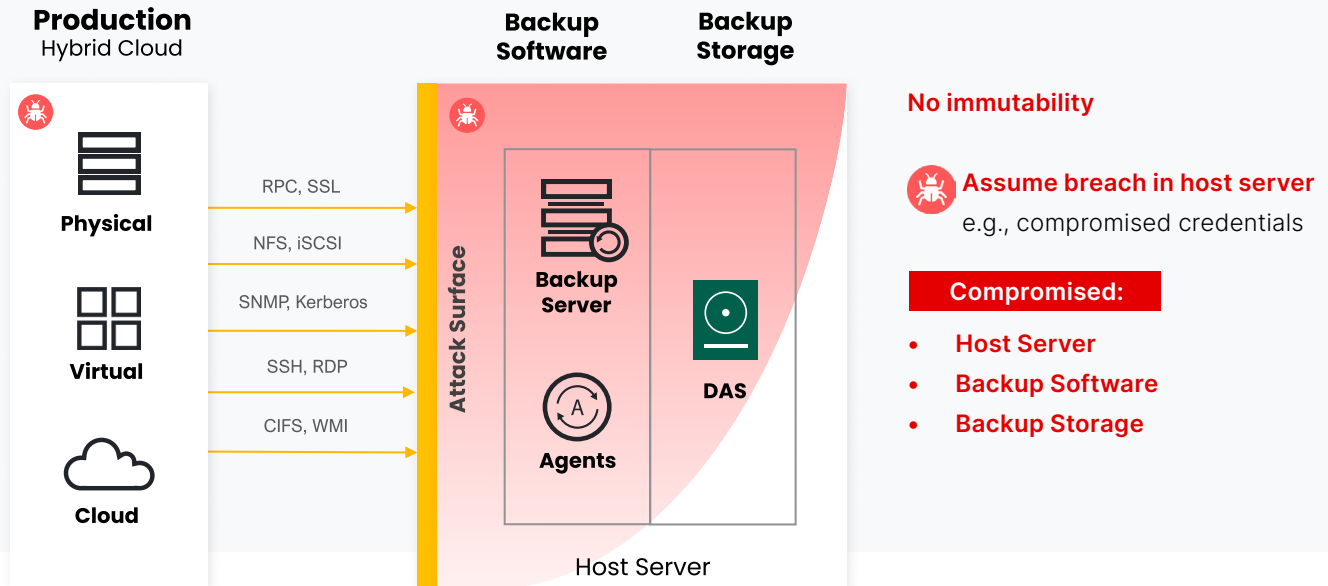
Here's why Ootbi's best for Veeam

- **Industry-standard S3 immutability, security and communication protocol supporting Veeam Data Platform V12 "direct-to-object" functionality.** Communication protocol over Smart Object Storage API (SOSAPI) with HTTPS ensures secure communication and encrypts all network traffic between Veeam and Ootbi.

- Open design and architecture.

- A hardened object storage appliance with **zero access** to the operating system that is third-party tested with constant security validation creates an impenetrable target for Veeam backup data.

- Veeam architecture and hardware form factor guarantees **separation between the Veeam Backup & Replication server** (Backup Software) and **Ootbi** (Backup Storage), with multiple resilience zones ensuring Zero Trust model is enforced.

Secure

S3 out-of-the-box Immutability

A hardened storage target with zero access to root

Separation of the Backup Software and Backup Storage layers

2. The Best Storage is Simple

Ootbi is an object storage appliance built for backup and, even more specifically, for Veeam. It takes less than 15 minutes to configure, requires zero security and Linux expertise, and no additional setup or namespace adjustment is needed at the Veeam layer when scaled.

Here's why Ootbi's best for Veeam

- **No expertise required configuration.** Setup requires 3 IPs (two physical and one vIP for the S3 endpoint), a username, password, and MFA setup. That's it!

- **Additional nodes can be added in minutes** with automatic scaling and load balancing. No change to Veeam Namespace or Backup Repository configuration is required.

- **Supports Veeam Smart Object Storage API (SOSAPI)** for simplified management.

- Notifications and updates are easily accessed from Object First servers ensuring the Linux kernel and our proprietary object storage software are secure and up-to-date with QA-tested patches, mitigating the impact of zero-day vulnerabilities and exploits.

👍
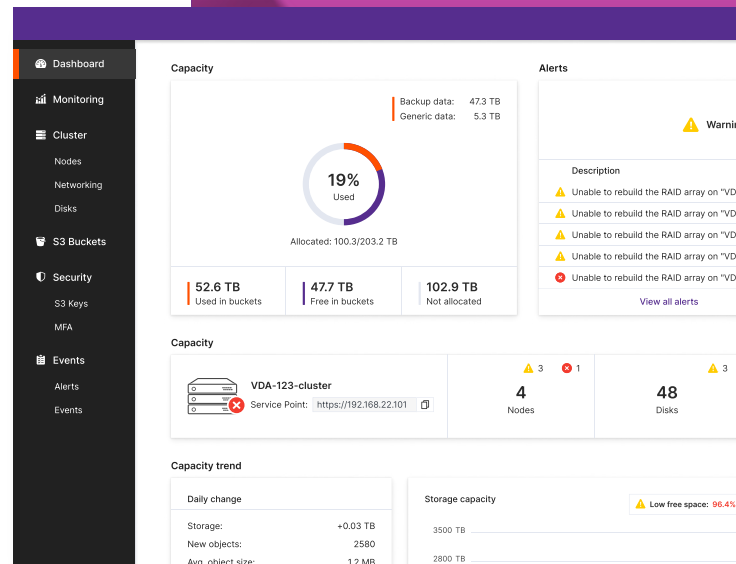
Simple

NO security expertise required
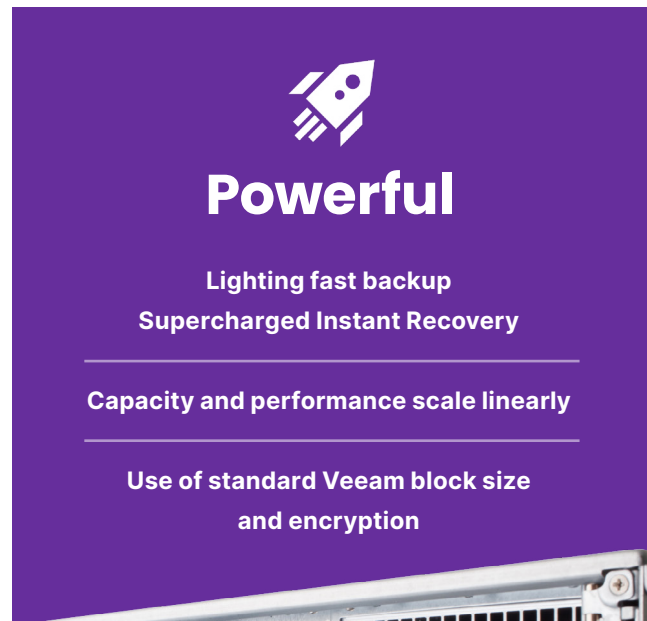
---

15 minutes to deploy and scale

Updated and optimized automatically by the vendor

3. The Best Storage is Powerful

Ootbi is an object storage appliance built for the backup use case and, even more specifically, for Veeam and Veeam Instant Recovery. Capacity and performance scale linearly when adding additional nodes, supporting backup speeds up to 4.0 gigabytes per second with up to half a petabyte of storage space. Ootbi was designed to empower Veeam Backup & Replication and supports Veeam's standard block size and encryption by default.
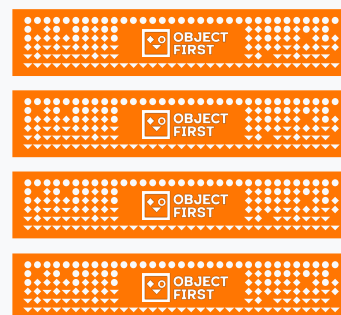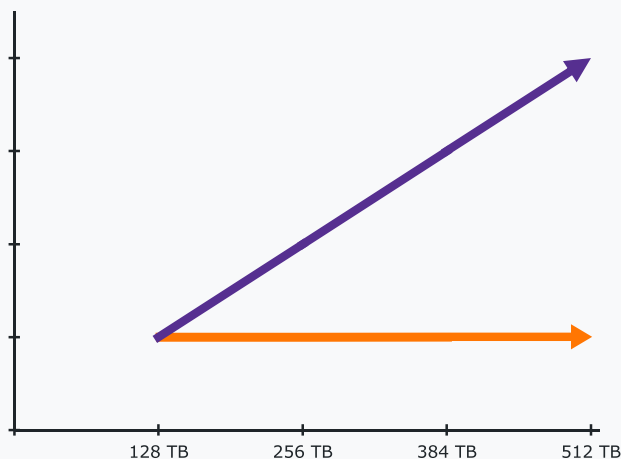
Here's why Ootbi's best for Veeam

- **Instant Recovery tested at scale with up to 80 VMs running on a 4-node cluster.**

- Two dual-port 10Gb NICs (for a choice of T-base or SFP+) parallelize incoming data streams landing on an enterprise-grade NVMe that automatically load balances objects to the RAID 6 array. This **delivers primary storage ingest speeds** without paying for an all-flash device that **scales linearly as nodes are added.**

- **Object storage engineered explicitly to ingest and secure Veeam data** means no additional and unnecessary features or functionality to impact performance.

Powerful

Lighting fast backup Supercharged Instant Recovery

Capacity and performance scale linearly

Use of standard Veeam block size and encryption

Performance + Capacity   Management Overhead

128 TB per node
512 TB Total Usable Capacity
4.0+ GB/s Performance

128 TB   256 TB   384 TB   512 TB

Object Storage is Best for Backup and Recovery

Object storage is best for the data backup and recovery use case. Object storage's S3 native immutability, unlimited scalability, lower cost of storing large volumes of data, seamless on-premises-to-cloud data copy, simplified management, reliability, and availability made it our only choice when we built Ootbi.

Object storage is best for backup and recovery use cases because:

- **Immutability:** S3 native Object Lock. Secure, resilient, and purpose-built means data is isolated and untouchable.

- **Scalability:** Object-based systems anticipate horizontal scalability, which never sacrifices performance for capacity.

- **Up-to-Date:** Bugs, quirks, or limitations of a traditional file system are absent in object-based architectures.

- **On-Prem-to-Cloud:** Secure and seamless on-premises-to-cloud data copy in S3 format with no overhead.

- **Reliability:** The S3 protocol has guaranteed data delivery (unlike SMB or NFS), so businesses get end-to-end data reliability.

- **Availability:** Natively solves many of the availability needs organizations consider when implementing backup storage and the 3-2-1 backup rule.

Other object storage vendors have designed their on-premises appliances for a different use case — distributed web-scale containerized enterprise applications — and optimized their S3 implementations to write small amounts of data in a large number of containers. Later, they retrofitted their solutions for the Data Backup use case, keeping the unneeded features and complexity. These solutions were not designed and optimized for Data Backup. Ootbi, on the other hand, has been specifically designed for the Data Backup use case, where large amounts of data need to be written in and read from one place. That is why Ootbi's object storage is simple and powerful for Veeam backup data.

OBJECT FIRST

Best for Veeam Backup

Ransomware-proof and immutable out-of-the-box, Ootbi by Object First delivers secure, simple, and powerful backup storage for Veeam customers. The appliance can be racked, stacked, and powered in 15 minutes.

Ootbi is built on Zero Trust principles and delivers S3 native immutable object storage designed and optimized for unbeatable backup and recover performance. Eliminate the need to sacrifice performance and simplicity to meet budget constraints with Ootbi by Object First.

When you think about Veeam, think about Object First.