OBJECT FIRST

White Paper

Absolute Immutability

The Ultimate Ransomware Defense

veeam Ready Repository

veeam Ready Object Immutability | SOSAPI IAM/STS

Immutable backup storage Your only guaranteed path to recovery after a ransomware attack

Ransomware has emerged as the most pressing cybersecurity threat—in fact, 66% of organizations have experienced at least one ransomware attack in the past two years. With the potentially devastating consequences of an attack, this is no longer just an "IT problem," but must command the attention of CIOs, CEOs, and boards of directors who hold organizational—and increasingly legal—responsibility for business continuity.

To defend against ransomware, organizations must adopt a modern, multi-layered cybersecurity strategy grounded in Zero Trust principles. This includes deploying a comprehensive suite of tools and solutions such as firewall, malware detection, threat hunting, access management, endpoint/extended detection and response, and more.

However, the stark truth remains: no system is impenetrable, no matter how robust your defenses are. That's why it's critical to **assume breach** and **prepare for recovery**.

The only guaranteed path to recovery after a ransomware attack is to maintain completely reliable backups. In this paper we introduce a new concept—'Absolute Immutability'—which means data cannot be altered or deleted under any circumstances ensuring that even if your production and data backup systems or access controls are compromised, your data remains safe.

Without Absolute Immutability, many organizations remain vulnerable. While 96% of ransomware attacks now target backups in addition to primary systems, 41% of organizations admit they do not use immutable storage for backup data.

This paper describes how Absolute Immutability is the ultimate defense against ransomware, and provides practical guidance for business and IT leadership teams on adopting it for reliable business resilience.

*ESG Research, 2025

50%

of organizations took more than 6 days to recover after a ransomware attack*

96%

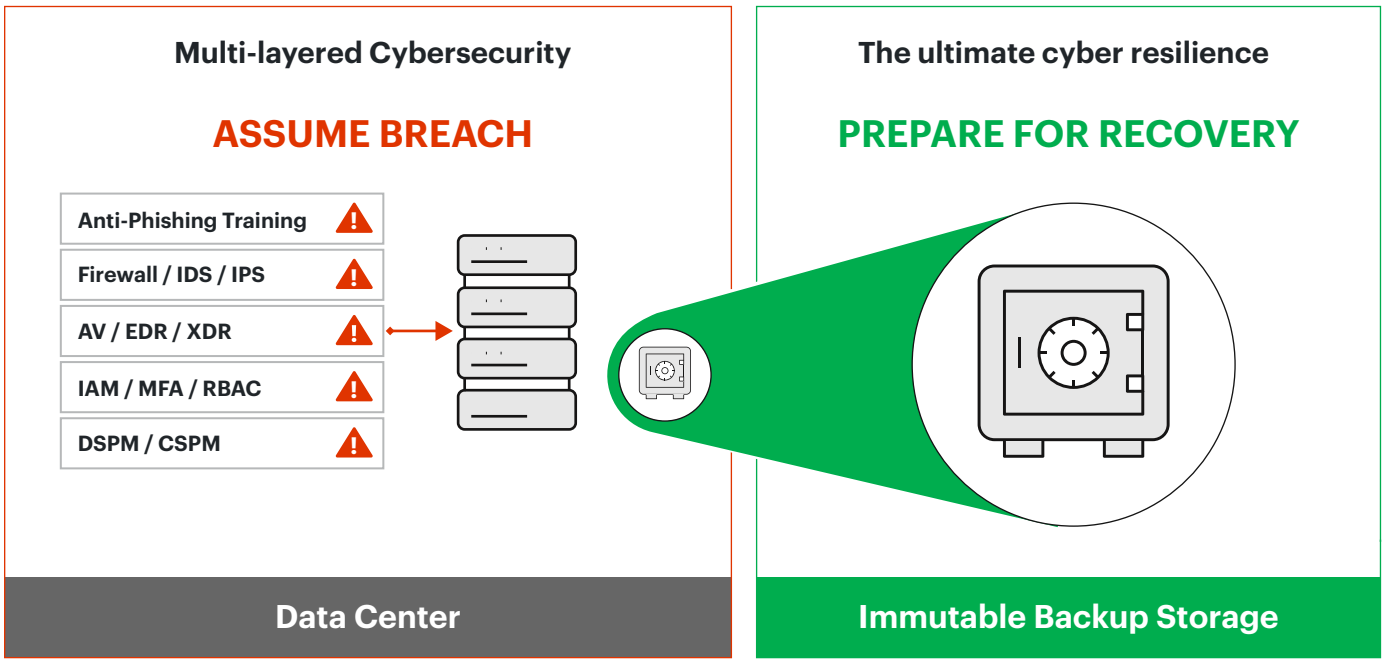
of ransomware attacks now target backups in addition to primary systems*

41%

of organizations do not currently use immutable storage*

Absolute Immutability

Immutable backup storage—the ultimate ransomware defense



When—not if—a breach happens, and your business, reputation, and career are on the line, immutable backup storage is your ultimate ransomware defense.

Key Concepts

What is Immutability?

In its simplest definition, immutability ensures that data cannot be altered or deleted once recorded, providing a secure means of safeguarding critical data. However, this definition does not account for the complexity of implementing immutability and the hidden exceptions and loopholes. This is why organizations must ensure they have ABSOLUTE Immutability.

What is ABSOLUTE Immutability?

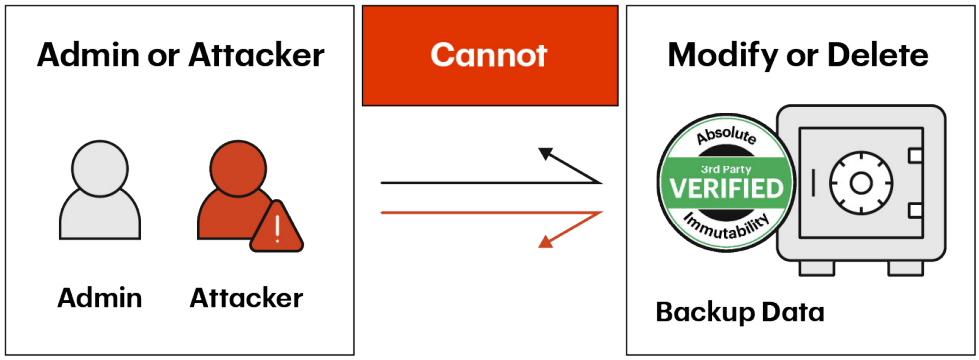
Absolute Immutability means that even the most privileged admin or attacker with access to backup storage cannot modify or delete data. This can only be achieved using a backup storage system that is "secure-by-design" with Zero Access to perform destructive actions, and this Zero Access must be verifiable with third party testing.

Why emphasize this? Because as we'll demonstrate, not all solutions that claim immutability really deliver it.

Absolute Immutability:

Zero Access to perform destructive actions

Third-party tested & verified

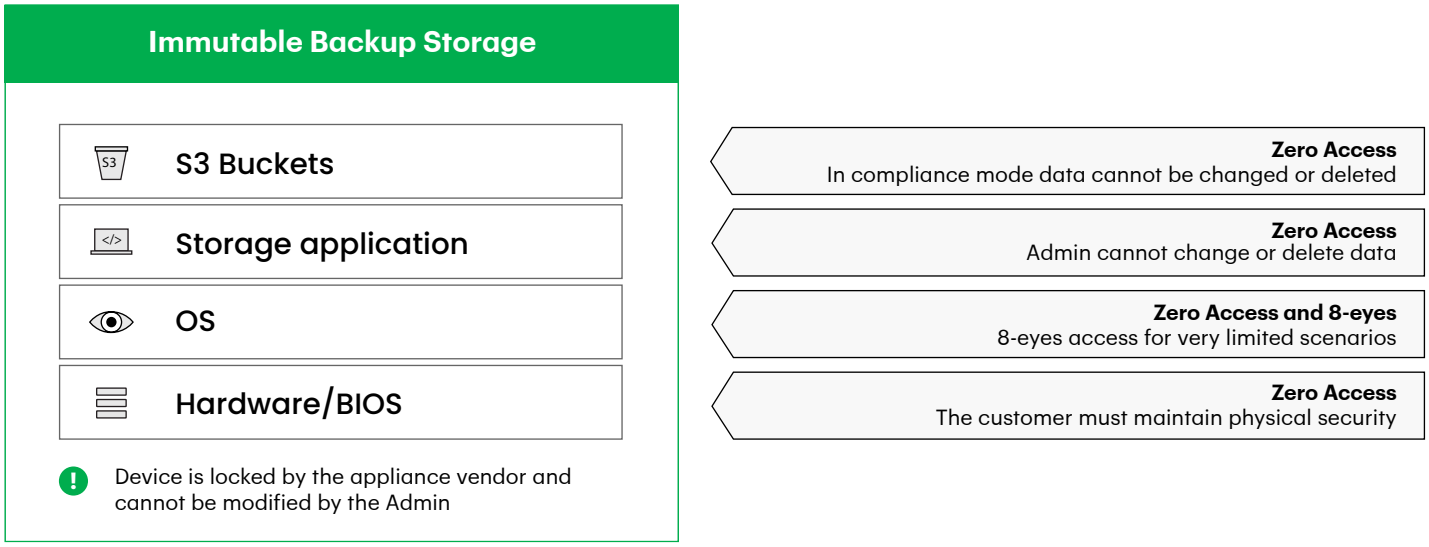


Extending Zero Trust to Zero Access

When a breach occurs, the administrator's credentials or privileges are compromised by the attacker—whether through phishing, social engineering or zero-day software vulnerabilities. Least Privilege Access, one of the key tenets of Zero Trust, limits administrator permissions—while Zero Access goes further by removing an administrator's ability to perform any destructive action, thereby protecting from attackers with administrative privileges or rogue insiders. In case of S3 object storage backup appliances, Zero Access achieves this by:

- Not allowing bucket or object deletion via compliance mode protection.
- Blocking root-level access to the operating system and backup storage application, ensuring immutability settings cannot be overridden.
- Eliminating the option to unilaterally perform factory resets—whether customer or vendor based—to prevent wiping out the system.
- Restricting BIOS access to physical-only modifications, preventing tampering with boot processes or security settings.
- Only allowing service procedures and updates to firmware and software to be provided by the vendor, and delivered in a way that preserves zero access to destructive actions.

Zero Access throughout backup storage



Eight-Eyes Protocol

Vendors taking a Zero Access stance also implement multi-person approval protocols to prevent unilateral destructive actions such as device resets, changing security or retention settings, or extraordinary service operations. Many already follow the four-eyes security principle, requiring two individuals—one from a customer and another one from a vendor—to approve critical operations such as these. However, verification is generally left up to individuals on the customer side—with a risk that compromised admin credentials could be used to circumvent this process.

For immutable backup storage, this should be extended further into an Eight-Eyes Protocol—requiring two customer-side individuals and two vendor-side staff, ensuring legitimacy before execution of a potentially destructive action. Additionally, identity verification must be enforced before finalizing any security-impacting decision.

Practical Implementation

Achieving Absolute Immutability through Zero Access requires adherence to three core principles:

Absolute Immutability	Unverified Immutability
1. S3 Object Storage	Proprietary Storage
2. Zero Time to Immutability	Time-Delayed Immutability Snapshot-Based Immutability
3. Target Storage Appliance	Integrated Appliance Dedupe Appliance Self-Managed System DIY Storage System

1. S3 Object Storage

Only S3 object storage provides inherent security, with native immutability built directly into its protocol and APIs.

This foundational design ensures that once data is written, it cannot be altered or deleted. In contrast, traditional block and file storage systems lack native immutability and instead rely on proprietary, bolt-on solutions that were added as an afterthought.

S3 object storage is based on an industry-standard, open architecture that aligns with IT security best practices. Unlike proprietary systems that depend on obscurity and cannot be independently verified, S3 embraces transparency through open standards. This approach fosters stronger security, broader compatibility, long-term reliability, and seamless integration with modern backup solutions like Veeam.

Proven across industries, S3 object storage has demonstrated its security and reliability at enterprise scale, with its capabilities continuously validated through real-world deployments and third-party testing.

Thanks to its native features, open design, and protocol-level immutability, S3 object storage stands alone as the only solution capable of delivering Absolute Immutability—a critical foundation for building a resilient, verifiable backup storage strategy.

Object Lock and Versioning

Object Lock prevents stored objects from being modified or deleted for a defined retention period—ensuring that even if bucket credentials are compromised, data cannot be altered or deleted. At the same time, versioning preserves multiple immutable iterations of data, providing multiple recovery points and allowing previous versions to be safely examined after a cyberattack to pinpoint when and where the infection occurred.

Compliance Mode

S3 object storage supports two mechanisms for immutability: Compliance Mode and Governance Mode. With Compliance Mode, retention periods are strictly enforced—even administrators cannot modify or delete protected data until the retention period expires. This ensures Absolute Immutability.

Governance Mode, on the other hand, poses serious security risks and should be avoided. While it offers administrative flexibility, it allows privileged users to override Object Lock settings, potentially shortening or removing immutability protections. If an attacker gains administrative access—whether through compromised credentials or insider actions—Governance Mode enables them to disable immutability and destroy backup data.

Despite some vendors recommending Governance Mode for its convenience, we strongly advise against using it. The flexibility it provides comes at the cost of security, undermining the very purpose of immutability.

For organizations that prioritize data integrity, regulatory compliance, and ransomware resilience, Compliance Mode is the only acceptable choice. It ensures that immutability cannot be bypassed—not by administrators, not by attackers, and not by mistake—making it the foundation of a truly secure and verifiable backup strategy.

End-to-End Encryption

When backup data in object storage is immutable, data can still be exfiltrated and read by anyone with access to S3 bucket credentials during a compromise. To eliminate this risk, all backup data must be encrypted the moment it is created—before it is sent to storage.

Data protection and privacy must begin when the data is read from production. Veeam supports and recommends as best practice end-to-end encryption with rotating keys, meaning that encryption keys change every backup session. This prevents data exfiltration even in the event of a security breach involving bucket access.

Dedupe appliances are NOT secure from exfiltration attacks!
Deduplication storage vendors require disabling end-to-end encryption, because rotating-key encrypted data cannot be effectively deduplicated or compressed.

Sacrificing data security to enable possible storage optimizations is never an acceptable trade-off. Protecting backup data from unauthorized access should always be the priority.

Third-Party Security Testing

When backup data in object storage is immutable, data can still be exfiltrated and read by anyone with access to S3 bucket credentials during a compromise. To eliminate this risk, all backup data must be encrypted the moment it is created—before it is sent to storage.

Data protection and privacy must begin when the data is read from production. Veeam supports and recommends as best practice end-to-end encryption with rotating keys, meaning that encryption keys change every backup session. This prevents data exfiltration even in the event of a security breach involving bucket access.

Absolute Immutability requires more than vendor claims—it must be independently verified. However, third-party independent testing is only possible when assessments are conducted against industry-standard open protocols.

Proprietary systems cannot be independently tested and verified. They represent a "Black Box" system requiring a customer to trust the vendor's security claims.

S3 object storage, with its open design and architecture and fully documented API, allows independent security researchers, auditors, and security teams to rigorously test immutability, access controls, and resilience under real-world attack conditions.

Independent test reports proving security should be a prerequisite for organizations seeking Absolute Immutability, although few vendors have conducted such testing—and some vendor license agreements expressly prohibit independent testing.

Without S3 object storage and its unique capabilities for enabling and enforcing data security, there can be no Absolute Immutability.

2. Zero Time to Immutability

Ensuring that backup data is immutable from the moment it is written is critical for preventing unauthorized alterations, maintaining data integrity, and defending against ransomware. The proven and most secure way to achieve this is through S3 versioning combined with Object Lock, which enforces immutability at the time an object is created in the storage system. This eliminates the risk of tampering, malware injection, or deletion—even in the event of insider threats or credential compromise.

In contrast, legacy storage solutions, designed in the pre-ransomware era, lack native immutability in their core architecture. To compensate, many vendors have attempted to bolt on immutability using various workaround techniques—none of which offer the same level of protection.

Not immutable: time-delayed “immutability”

Some storage solutions—such as deduplication appliances or DIY backup setups (where admins deploy, configure and maintain a backup repository themselves)—initially write backup data to a mutable landing zone or temporary file system. Immutability is only applied after the backup job completes. During this window, the data remains fully mutable and exposed to risk. An attacker could exploit this gap to inject malware or tamper with the data before immutability is enforced, compromising the integrity of the backup.

Not immutable: snapshot-based “immutability”

Traditional storage types like DAS (Direct Attached Storage), JBOD (Just a Bunch of Disks), NAS (Network Attached Storage), and SAN (Storage Area Network) do not support native immutability. Instead, vendors simulate immutability using snapshots: point-in-time copies that can be rolled back if needed. However, snapshots do not provide Absolute Immutability. They are created after data is written and reside on the same storage system as the primary data. This means a successful attack on production storage can also delete or corrupt both the live data and its snapshots.

3. Target Storage Appliance

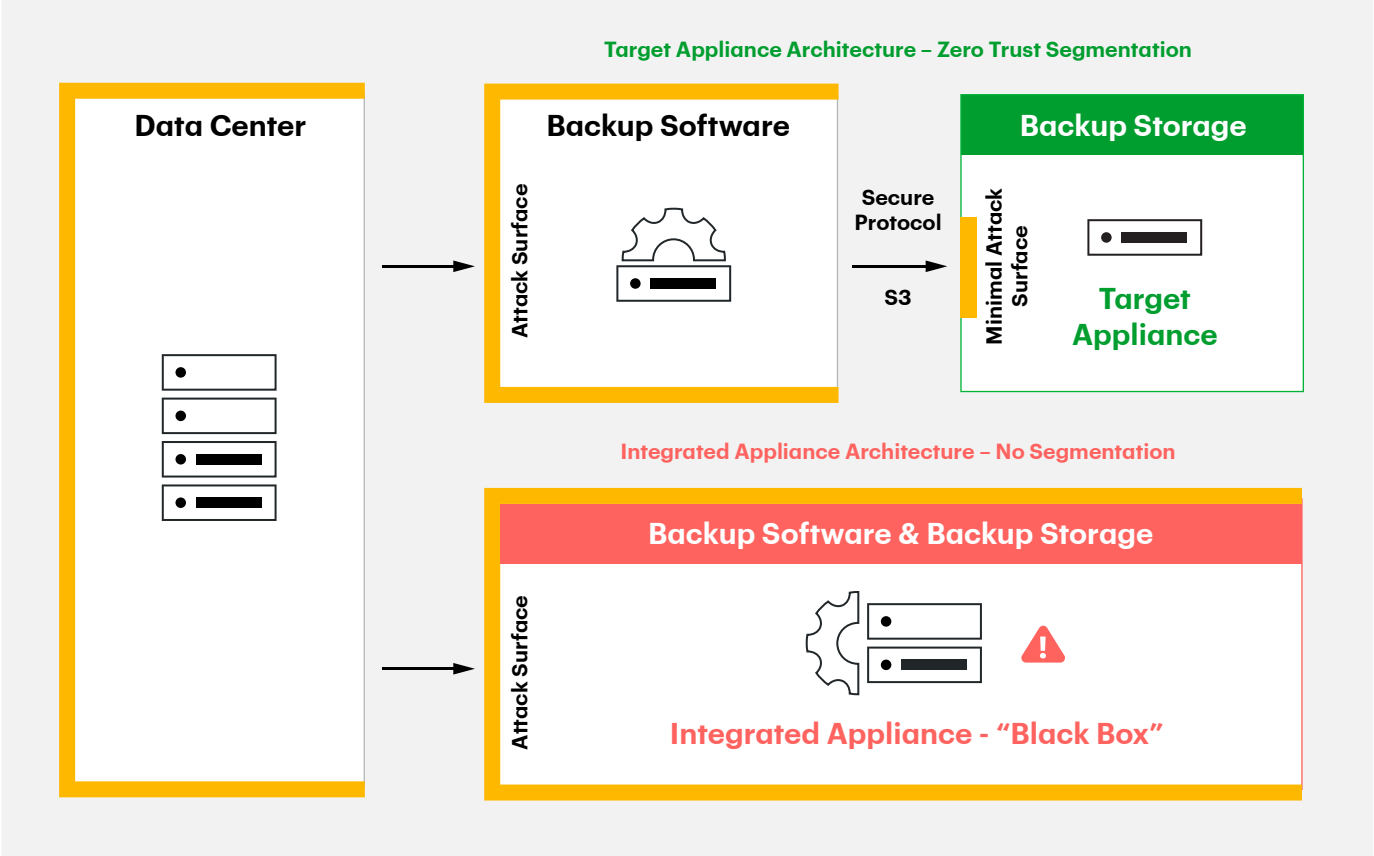
Purpose-built backup storage appliance means a standalone storage device that is configured and optimized for storing backup data. There are two types: Integrated Appliances, which combine backup software and storage in a single system; and Target Appliances, which provide a turn-key storage device for external backup software such as Veeam.

Separation of backup software and backup storage

A fundamental requirement for Absolute Immutability is the strict separation of backup software and backup storage. This separation is a requirement of the Zero Trust Data Resilience architecture developed by Veeam and Numberline Security. Proper segmentation as supported by a target appliance reduces the storage attack surface by ensuring that backup data is physically isolated from the backup software that manages it according to a defined, documented protocol; and that multiple backup copies remain separate from each other in different resilience zones. This ensures that even if credentials are stolen, attackers cannot modify or delete backup data, and safeguards remain in place against system failure or other disasters.

Only a target appliance built on S3 with Zero Access principles can properly achieve this separation.

Target vs integrated appliance



Not verifiably secure: integrated backup appliance

Integrated backup appliances do not provide Absolute Immutability because, upon breach, an attacker will have full access to the backup software and storage. The attacker may be able to modify, delete, or render backup data inaccessible. In other words, the blast radius of an attack would include the full backup and recovery system.

This approach places a large amount of trust in the vendor's proprietary file system immutability. It is impossible to know, or test, what is happening inside the "Black Box." Only a target appliance built on the open S3 protocol can be independently tested, making it verifiably secure.

Not secure: Do-it-Yourself (DIY) backup storage system

In a DIY setup, backup storage is either manually assembled by installing storage software on self-provisioned hardware or delivered pre-installed on a general-purpose server. While the former offers flexibility and the latter convenience, both approaches leave critical operations—such as daily monitoring, patching, servicing, and lifecycle management—entirely in the hands of the customer.

As a result, each deployment becomes a unique, often undocumented environment with no standardized support or assurance of proper network segmentation, configuration consistency, or operational best practices. This lack of uniformity introduces significant vulnerabilities while the high level of expertise in both Linux and cybersecurity means this resource-intensive approach can also create key person dependencies.

Not secure: DIY backup storage system deployed as a VM

Deploying a DIY backup storage system within a virtual machine introduces additional layers of risk. In this setup, immutability is enforced only through software controls inside the VM—not at the hardware or storage infrastructure level. This makes the system inherently more vulnerable. If an attacker gains access to the virtualization layer or the underlying physical storage, they can easily delete, reassign, or manipulate the entire backup VM and its virtual disks—often with just a few clicks.

Only a purpose-built, turn-key backup S3 target appliance can verifiably deliver Absolute Immutability, with correct segmentation and enforced security and lifecycle operations at the system level. This eliminates the risks and inconsistencies common in DIY deployments and the "trust us" approach of integrated "Black Box" appliance vendors.

Conclusion

In summary, Absolute Immutability is essential for safeguarding backup data against increasing ransomware threats. It protects sensitive information, ensures compliance with regulations, and maintains data integrity during legal processes—but most importantly, it ensures recoverability and resilience. If 'immutable' data can be overwritten by a backup or storage admin, a vendor, or an attacker, then it cannot be considered an absolutely immutable storage solution.

Understanding the core concept of Absolute Immutability will help separate secure backup systems from empty vendor claims.

This core concept—and the definition of Absolute Immutability—is allowing Zero Access to perform destructive actions. Nobody—even the most privileged admin or attacker with access to backup storage—can modify or delete data.

Practical implementation of Absolute Immutability requires adherence to three core principles:

- S3 Object Storage: A fully documented, open standard with native built-in immutability that enables independent penetration testing and verification.
- Zero Time to Immutability: Backup data must be immutable the moment it is written.
- Target Storage Appliance: A dedicated target storage appliance segments storage from backup software, and removes the risks associated with DIY self-managed backup storage during operations—particularly during setup, updates and maintenance. It requires little-to-no security expertise from a customer and shifts full responsibility to a vendor.

By following these three principles, organizations can assure Absolute Immutability and thereby ensure that whatever happens—ransomware, insider threats, or credential breaches—backup data remains protected and recoverable.

About Object First

Ransomware-proof and immutable out-of-the-box, Object First delivers secure, simple, and powerful backup storage purpose-built for Veeam. The appliance can be racked, stacked, and powered in 15 minutes. Secure-by-design and secure-by-default, Object First helps Veeam admins implement a Zero Trust Data Resilience architecture for unbreakable backup and recovery.

Simply Resilient for Veeam

1.0_20251118

OBJECT FIRST