WHITEPAPER

Why Immutable Storage is the Ultimate Solution to Data Protection

JAMES PENDERGRASS
SALES ENGINEER,
NET3 TECHNOLOGY

NET3 TECHNOLOGY
LEADING NATIONAL CLOUD SERVICES PROVIDER

About the Author

James has designed and implemented robust and secure data protection strategies for many years at Net3. From initial contact with the customer, James dives into each business environment to understand the current technical requirements and what each business needs to achieve with data protection and endpoint security. James' mission is to provide solutions that help shrinking IT departments maintain operational and information security while keeping additional workloads to a minimum.

By now, everyone knows the importance of backing up your data. But with cybersecurity threats evolving and increasing, how can we ensure our backup data is secure?

We rely on backups to keep our data secure in the event of a disaster event such as ransomware, human error, natural disasters, etc. Unfortunately, we can no longer assume data backups are secure and protected from attacks.

We are going to break down how immutable storage is the ultimate solution to keeping our backup data secure by explaining:

- Why backups are at risk
- What immutable storage is
- How immutable storage works
- Immutable storage options

Immutable Storage

The ultimate solution to secure, reliable data protection

With the importance of backups in a business, keeping your backup data secure is vital. Backups contain sensitive data from each of your servers which includes accounting information, human resources data, and even health records. A way to protect this data is to make sure that your backup data is encrypted at rest.

1 in 4

organizations were able to recover from their ransomware event by recovering from backups instead of paying the ransom

But what if a security breach allows an attacker to brute-force that encryption password? All of that sensitive data is now available to be moved, changed, or even deleted. This could mean that, by the time you realize that your environment has been compromised, the attacker has already gained access to your backups and possibly deleted those backups, leaving you no way to restore your data. Unfortunately, this is something that happens way too often when an attacker gains access to a business' environment.

Fortunately, there is a way to protect against this – immutable storage. With immutable storage, you are able to set a timeframe where the data on that storage is not able to be modified or deleted. For example, a timeframe of 7 days can be set so that, for those 7 days, no backup files can be changed. So, if an attacker were able to get access into your backup solution, decrypt your backup data, and gain access to the backup storage, the data within those 7 days could not be touched. While these backup files cannot be modified, you would still retain the ability to restore servers from those backup restore points. This is all able to happen because files in immutable storage are stored in a 'write-once, read-many' format.

Immutable storage is the ultimate solution to ensure your data is completely protected. It can protect your data against ransomeware, even if the attacker is able to circumvent file permissions to gain access to the backup storage. It can protect your business from things that may not be intentionally malicious, like accidental file deletion. Immutability can even be used to ensure data authenticity and make sure data is not tampered with and ensures the integrity of files. Immutability also helps with keeping up with regulatory requirements, such as HIPAA and SEC regulations.

With businesses under constant attack from ransomeware attackers, backups are essential for businesses. Immutable storage gives another layer of protection for your backups by not allowing that data to be modified, encrypted by another process, or deleted. According to Veeam's 2022 Ransomware Trends report, immutable storage was the #1 contributor to organizations being able to successfully recover from a backup instead of paying the ransom.

The three most important contributors to being able to successfully recover from a ransomware event using backups instead of paying the ransom are:

1. Immutable/air-gapped backup repositories
2. Verifiably recoverable and assuredly "clean" data
3. Orchestrated workflows for recurring testing & reducing the time of remediation

Immutable Storage Options with Net3 Technology

At Net3, we offer immutability with both Acronis and Veeam. In these products, our customers are able to specify the amount of time that the backups stay in an immutable state. One thing to keep in mind with immutable storage is that it will take precedence over the retention policy if the retention policy is less than the immutability time frame. For example, if you have the retention of your backups to be 5 days, but immutability is set at 7 days, the immutability will override the retention rate and keep backups for 7 days, which will result in additional storage being used. With our Disaster Recovery product, Zerto, there is no way to access the data points and delete checkpoints per the product design.

To learn about Net3 immutable storage options, click below or email sales@n3t.com

Acronis **Learn more**

veeam **Learn more**

Zerto **Learn more**

Net3 Technology is a leading Cloud Services Provider offering Backup, Disaster Recovery, Infrastructure-as-a-Service (IaaS), Cybersecurity, and Ransomware Protection. Our wide range of offerings paired with our customer support provides customers with the freedom of choice and ensures cloud confidence for IT teams nationwide.