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 the initial customer contact, James dives into each business environment to understand the current technical requirements and what each business needs to achieve in 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 as cybersecurity threats evolve and increase, how can we ensure our backup data is secure?

We rely on backups to keep our data secure in the event of a disaster, such as ransomware attacks, human error, or natural disasters. 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

Copyright @ 2022

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 your environment has been compromised, the attacker has already gained access to your backups and possibly deleted them, leaving you no way to restore your data. Unfortunately, this happens way too often when an attacker gains access to a business's environment.

Fortunately, there is a way to protect against this – immutable storage. With immutable storage, you can set a timeframe during which the data in that storage cannot be modified or deleted. For example, a 7-day timeframe can be set so that, during those 7 days, no backup files can be modified. So, if an attacker were to gain access to your backup solution, decrypt your backup data, and access the backup storage, the data within those 7 days could not be touched. While these backup files cannot be modified, you can still restore servers from those backup restore points. This is all possible 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 ransomware, even if the attacker can circumvent file permissions to access the backup storage. It can protect your business from unintentionally malicious events, such as accidental file deletion. Immutability can even be used to ensure data authenticity and make sure data is not tampered with, and ensure the integrity of files. Immutability also helps with keeping up with regulatory requirements, such as HIPAA and SEC regulations.

Copyright @ 2022

With businesses under constant attack from ransomware, backups are essential. Immutable storage adds another layer of protection to your backups by preventing that data from being modified, encrypted by another process, or deleted. According to Veeam's 2022 Ransomware Trends report, immutable storage was the #1 factor in organizations successfully recovering from a backup rather than 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

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 set your backup retention to 5 days but immutability to 7 days, immutability will override the retention and keep backups for 7 days, resulting in additional storage usage.

To learn about your immutable storage options with Net3 Technology, contact us by emailing sales@n3t.com. Let's get your business protected today!

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

Copyright @ 2022