NSP
SECURE YOUR FUTURE

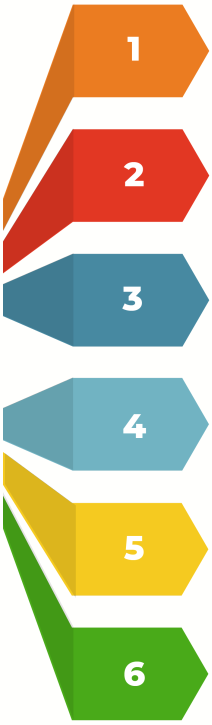
IMMUTABLE BACKUP

Protecting against malicious attacks across backup databases - Data backups alleviate the operational pain encountered due to software/hardware breakdown, data corruption, accidental data deletion, human errors, cybersecurity threats, and natural calamities. However, recent cyber-attacks specifically targeting backup databases has raised concerns around backup safety. As a result, the best practice today is to deploy immutable backup solutions that hackers cannot modify, encrypt, or delete, even if they have gained full admin access to your backup server.

What is ransomware - Ransomware is a type of malware or software code that is designed to block access to your data. This is typically achieved by encrypting that data so your files are unable to be opened or accessed in any way. Some variants change file extensions, while others simply encrypt files. Hackers then demand a ransom (often in bitcoin) in exchange for decryption keys, or a decoder to restore access to your data. It’s the digital version of kidnapping – your data is held hostage unless, and until you pay for its safe return.

How NSP secure backup protects - NSP Secure Backup ensures your backup data is fixed, unchangeable and unable to be deleted. Once you have stored an immutable backup, it cannot be altered or changed and is impervious to new ransomware infections. By keeping an archive of immutable backups, you are implementing best practice protection and recovery.

6 reasons you need to make your backup immutable



1. **All Data Is Highly Vulnerable -** Data is king and everyone wants to get their hands on it, especially cybercriminals. Data can fall victim to tech failure, ransomware attacks, insider threats and viruses resulting in downtime, financial loss, lost opportunity, legal repercussion, reputational damage, and diminished trust.

2. **Stay compliant -** Immutable backup helps organisations meet data compliance regulations by creating malware-resistant backups of your critical systems and data which helps ensure provably accurate copies of historical data are retained.

3. **Protection against Tech Failure -** Malware and viruses, unexpectedly crashes and power failures can result in data loss. Subsequent downtime, interruption, productivity loss and low morale can follow. Avoid these scenarios with Immutable data backup couple with a robust recovery plan.

4. **Guard against Human Error and Insider Threat -** All humans are prone to error, and employees may lose their devices, damage hard drives or even delete essential files intentionally or unintentionally.

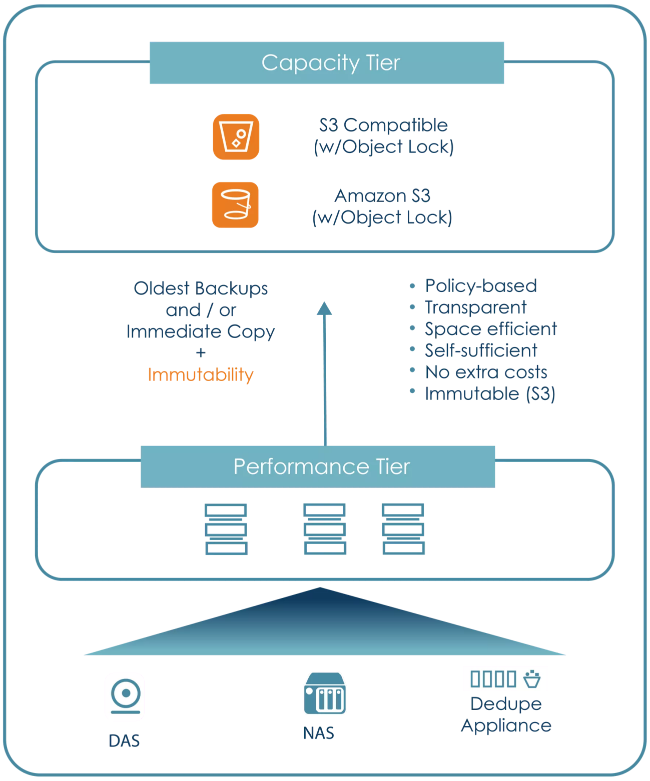
5. **Stay Safe from Natural Disaster -** Earthquakes, fires, and floods can impact your business technology systems. A cloud-based immutable backup, air-gapped from the primary storage, offers instant data protection from natural disasters yet is still immediately accessible.

6. **Support Remote Work -** Remote working is the new normal, so locally stored data will be of no help to geographically dispersed employees. Harnessing immutable cloud data backup and recovery services will ensure essential business data safety regardless of data origin.

Immutable backup components

The hardened repository in Veeam Backup & Replication V11 provides the air-gap or immutability we need. It merely means that the backup files cannot be changed or deleted from the Linux server's storage without having root access. Veeam does not require that kind of access to function, which means the Veeam backup fabric users and accounts cannot delete backups.

Air gapping - If hackers can get into your network environment, you will need something to stop them from accessing your operating system and making changes. An air-gapped solution ensures the connection between a) your backup or environment and b) your backup device is separated. The account will only have write permissions, meaning its sole purpose is to let new files through. Furthermore, we can lock it down in the firewall so it doesn't have internet traffic or talk to the internet.



Example Immutable Architecture

Veeam Scale-Out Backup Repository (SOBR) - The SOBR solution, partnered with Capacity Tier, makes sure to write backups into object storage on any platform that supports object store. AWS S3 or select S3-compatible storage also provides access to Object Lock, enabling backup data to be stored as an immutable backup.

Multi-level Approvals - The backup is stored on the cloud and utilises controls that hinder the possibility of data deletion or modification without strict multi-level approvals.

Veeam ONE Monitoring - Veeam ONE allows users to monitor their environment to stay on top of suspicious or abnormal activities. The solution analyses CPU usage, datastore write rate, and network data transmission rate to identify abnormal activities. Any issues trigger the alarm and notify the user to inspect the machine in question.

Veeam SureBackup - The Veeam SureBackup is an automated solution that notifies the user of an unrecoverable system due to an undetected malware or ransomware infection. The solution automatically scans the existing backups for malware, providing protection at all stages of backup and recovery.

Veeam Secure Restore - The Secure Restore solution conducts a complete antivirus scan of older backups when restoring them. The virus definitions are always up to date and help recognize new and dormant viruses in data backups. This process prevents them from infecting the environment after restoration.