Immutability Is Not Enough Protection Against Cyber and Ransomware Attacks

By Andrew Glinka | April 2022

Cyber and ransomware attacks are at the forefront of business disruption concerns. To counter these threats, there are many cybersecurity and recovery solutions available, including immutable backups which are data copies that cannot be modified or deleted by unauthorized parties. Many vendors promote their immutable backup approach as being good enough for safe and secure data recovery. It's certainly better than nothing, but given today's fast-evolving threat environment, it's not enough.

Immutability Limitations

When considering ransomware and cyberattack protection, immutability is an important component of the backup and protection process, but it simply does not provide enough protection on its own. Many attacks can still thwart immutability within a production environment:

- System Clock Tampering can accelerate the expiration of backups
- Kernel Access via an unpatched vulnerability can allow root access to the underlying system
- Platform Corruption of a system's firmware or data can occur due to malicious Trojan code or spyware
- Hypervisor Changes – software-defined immutability in a Virtual Machine can be defeated by deleting the virtual disk at the hypervisor level

Any of these attack vectors can compromise an appliance's immutability, so any vendor solution based solely on immutability is vulnerable.

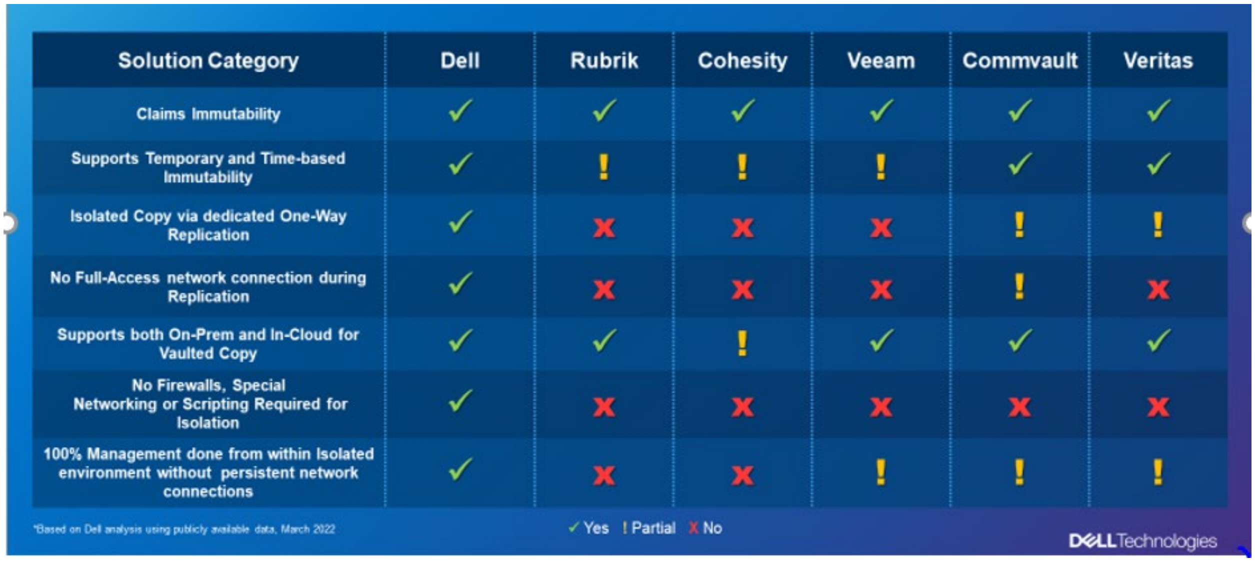
Inherent Advantages of True Isolation

Isolating a copy of your critical data will complement immutability by providing a separate layer of backup protection. However, understanding how isolation works is critical. Many solutions on the industry claim to have an "air gap" that provides isolation, but it's important to consider the ways various air gaps can still be compromised:

- Isolation via separate virtual networks in production - If attackers compromise the networking infrastructure, they can bridge the isolated network using the compromised channel
- Using a proxy device to control communication - Proxies typically lack hardening and are built on commodity hardware/software which are susceptible to operating system vulnerabilities
- Placing a firewall between two production units - Configuration rules allowing network traffic at prescribed times increases complexity, and firewalls can still be compromised allowing access to the storage environment

The inherent vulnerabilities for each of the above isolation methods can be eliminated by dedicating a physical link between production storage array(s) and a secure backup storage appliance for one-way replication. One-way replication uses a separate, dedicated 'vault' environment for ensuring *true* isolation of devices *and* data copies. Additionally, separating copied data from management layers inside the vault provides extra safeguarding and data security against external malware penetration.

Dell’s PowerProtect Cyber Recovery air gap vault features one-way replication and provides complete isolation in addition to immutability. The table below shows how our PowerProtect Cyber Recovery isolated vault architecture stands out from the competition:



Solution Category	Dell	Rubrik	Cohesity	Veeam	Commvault	Veritas
Claims Immutability	✓	✓	✓	✓	✓	✓
Supports Temporary and Time-based Immutability	✓	!	!	!	✓	✓
Isolated Copy via dedicated One-Way Replication	✓	✗	✗	✗	!	!
No Full-Access network connection during Replication	✓	✗	✗	✗	!	✗
Supports both On-Prem and In-Cloud for Vaulted Copy	✓	✓	!	✓	✓	✓
No Firewalls, Special Networking or Scripting Required for Isolation	✓	✗	✗	✗	✗	✗
100% Management done from within Isolated environment without persistent network connections	✓	✗	✗	!	!	!

*Based on Dell analysis using publicly available data, March 2022

✓ Yes ! Partial ✗ No

Immutability has its place and is a critical component for both storage arrays and backups. However, there are many ways immutability can be compromised, so it should not be solely relied upon for defense against cyberattacks. Adding a data vault with a strong physical and logical isolation design is a must for strengthening resiliency and protecting mission-critical data copies against malware, ransomware, cyberattacks, and insider threats.

If you’re interested in learning more about PowerProtect Cyber Recovery and how it can help protect and recover mission-critical backup data more reliably, securely and faster compared to other cyber security solutions, click on this link or contact a Dell Sales Representative or Partner today. Discover for yourself how PowerProtect Cyber Recovery’s true isolated vault design offers increased data protection and cyber resilience beyond what immutability alone can provide.