CENTRE FOR CYBERSECURITY BELGIUM

TLP:AMBER

Day, Month, 2024

IMMUTABLE BACKUPS

Table of contents

A. Executive Summary

The modern cyber threat landscape has become increasingly malicious and sophisticated, with adversaries launching targeted attacks against organizations' most critical asset: their data. These attacks range from ransomware campaigns, which hold data hostage for financial gain, to insider threats or the use of wiper malware, a software specifically engineered to permanently destroy data, render systems completely inoperable, and cause maximum disruption to an organization's operations. The defining characteristic that distinguishes wiper attacks from other forms of malicious software is their single-minded focus on destruction rather than financial gain.

Historically, organizations relied on traditional backup systems to recover from such incidents. However, these systems are now a frequent target themselves of attackers, who aim to compromise or destroy backups to ensure victims are unable to recover from the attack. Considering these evolving threats, it is important that organizations enhance their backup strategies to remain resilient to modern threats.

Immutable backups have emerged as a critical safeguard in countering advanced cyber threats. By design, immutable backups cannot be deleted or modified once written, offering a secure and irrefutable data restoration point even in the event of a successful cyberattack. Leading research firm Gartner emphasizes that immutable storage is now a "must-have" capability for enterprise backup and recovery. By integrating immutability into your backup strategy, your organization ensures rapid, precise recovery from disruptions while maintaining compliance with regulatory mandates and bolstering public trust.

To assist your organization in selecting and implementing the appropriate immutable backup solution, this document delves into the various methods available for achieving immutability like cloud-based solutions, on-premises hardware or magnetic tapes. Each method is analyzed with respect to its benefits and trade-offs, offering actionable insights into how they align in the organization's operational environments. Additionally, the document emphasizes the importance of adopting a layered approach to immutable backups, which combines multiple methods to eliminate single points of failure and increase resilience

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister
Rue de la Loi / Wetstraat 18 - 1000 Brussels
www.ccb.belgium.be

against sophisticated cyberattacks but also maintain operational day-to-day recovery needs. Finally, the document discusses critical factors to consider when evaluating backup providers, such as integration capabilities, retention policies, and cost efficiency, to ensure any chosen solution seamlessly fits within your existing IT infrastructure and compliance requirements.

Adopting immutable backups as part of a broader, layered data protection strategy not only strengthens your organization's capacity to withstand modern cyber threats but also ensures operational continuity, improves data restoration times, and protects public trust in the critical services your organization delivers.

B. What are immutable backups

An immutable backup is a type of data backup that, once created, cannot be altered, deleted, or modified in any way. This tamper-proof nature makes immutable backups an essential safeguard in defending against modern cybersecurity threats, such as ransomware attacks or unauthorized data tampering by malicious insiders. By ensuring data integrity and availability, immutable backups serve as a reliable last line of defense for organizations.

The concept of immutability is rooted in Write Once, Read Many (WORM) technology, a storage model where data is written to a medium once and can only be accessed or read thereafter. Originally associated with archival storage solutions like magnetic tapes or CD-ROMs, WORM-based systems were designed to preserve critical data for long periods while ensuring its integrity. However, advancements in technology have brought immutability to a wide range of modern storage solutions, including hard disk drives (HDDs), solid-state drives (SSDs), and even cloud storage platforms. Today, many cloud service providers offer WORM-compliant or immutable storage options, enabling organizations to adopt this technology without additional physical infrastructure or operational complexity.

Immutable backups are particularly effective as a defense against ransomware because they render the attacker's typical strategy of encrypting or deleting backups useless. Even if threat actors gain access to the backup environment, they cannot overwrite or remove data stored in an immutable format. For this reason, immutable backups are becoming a best practice in modern data protection strategies across industries, particularly those heavily regulated or highly targeted by cybercriminals, such as finance, healthcare, and government.

C. Implementation options

Cloud-Based Immutable Storage

Cloud-based immutable storage leverages the infrastructure of major cloud providers to create Write Once, Read Many (WORM) backups using built-in object locking capabilities. The three primary providers offering this technology are AWS, Azure, and Google Cloud. These services prevent data from being altered or deleted by any person or process, whether the threat comes from unintended actions or malicious activity.

From a security perspective, cloud-based immutable storage adds a critical layer of protection against cyberattacks, particularly ransomware. The technology ensures that once data is written to the cloud, it cannot be altered or removed until the retention period expires, regardless of who attempts to access it or what credentials they possess.

Benefits

Operational Advantages

Cloud storage offers exceptional scalability and accessibility that traditional on-premises solutions struggle to match. Organizations can expand their backup capacity virtually instantly without procuring hardware, waiting for delivery, or installing physical infrastructure. This scalability is particularly valuable for organizations experiencing rapid data growth or those with unpredictable storage requirements.

The automation inherent in cloud-based solutions significantly reduces operational overhead and the risk of human error. Immutability is enforced automatically by the cloud platform itself, meaning organizations don't need to rely on manual processes or human vigilance to maintain backup integrity. This automated enforcement provides continuous protection without requiring constant administrative attention.

Recovery operations benefit from faster access and continuous availability. Unlike tape-based systems that require physical retrieval and mounting, cloud-based immutable backups can be accessed immediately over the network. The speed of recovery depends primarily on network bandwidth rather than physical logistics, making it possible to restore critical systems quickly when needed.

Cost efficiency

The pay-as-you-go pricing model eliminates large upfront capital expenditures. Organizations avoid the costs associated with purchasing hardware, and they don't need to invest in facility infrastructure like power systems, cooling equipment, or physical data center space. This financial structure can be particularly attractive for organizations looking to preserve capital or those with limited initial budgets.

Drawbacks

Post-Implementation Cost Growth

Despite these advantages, cloud-based immutable storage presents several notable challenges. The cost structure, while eliminating upfront expenses, can become significant over time as data volumes grow. Cloud storage and the associated immutability features typically scale with data volume, meaning monthly costs increase proportionally with the amount of protected data. Organizations must also account for data transfer costs, particularly egress fees when recovering large datasets from the cloud. These costs can accumulate substantially during major recovery operations.

Technical Limitations

The reliance on network connectivity represents a fundamental limitation of cloud-based approaches. Both backup and recovery operations require reliable internet connectivity, which can be problematic during

widespread outages or in locations with limited bandwidth. For very large datasets, recovery speed may be slower than local alternatives simply due to the time required to transfer terabytes or petabytes of data over internet connections.

Vendor lock-in presents another consideration. Once an organization commits significant data to a particular cloud provider's immutable storage platform, migration to a different provider can be complex, time-consuming, and expensive. The proprietary nature of each platform's implementation means that switching vendors often requires re-architecting backup strategies rather than simple data migration.

Security Concerns

From a security perspective, it's important to understand that cloud-based immutable backups are not truly "offline" or air-gapped. Unlike physically disconnected tape cartridges, cloud backups always remain connected and accessible from the network. While immutability prevents alteration or deletion, the backups are still potentially vulnerable to attacks that compromise cloud credentials or exploit access control mechanisms. The security of these systems relies heavily on role-based access controls and authentication mechanisms, meaning a sophisticated attacker who gains sufficient privileges could potentially find ways to misuse the backups.

On-Premise Vendor Appliances

On-premises vendor appliances represent dedicated backup hardware systems with built-in immutability features that organizations deploy within their own data centers. Many of the major vendors are offering these appliances that combine physical hardware with embedded immutability software specifically designed for backup and recovery operations.

The fundamental architecture of these systems involves purpose-built hardware optimized for backup workloads, integrated with proprietary operating systems that have been hardened to reduce attack surfaces. Unlike general-purpose servers, these appliances are engineered from the ground up for data protection, incorporating features like inline deduplication, compression, and encryption alongside their immutability capabilities. The integration with existing backup infrastructure typically occurs through standard protocols and APIs, allowing these appliances to work within established enterprise backup workflows.

Benefits

Performance and Control

The performance of on-premise appliances often exceed what most other solutions can deliver. Local network speeds for backup and recovery operations typically reach ten gigabits per second or higher, enabling rapid protection of large datasets and fast recovery times when systems need restoration. This performance advantage becomes particularly critical during major recovery operations where every minute of downtime carries substantial business impact.

Operating independence from internet connectivity provides crucial resilience. Backup and recovery operations continue uninterrupted during internet outages, which is essential for organizations in locations with unreliable connectivity or those facing scenarios where internet access might be deliberately disrupted during an attack. The appliances function entirely within the organization's local network infrastructure, depending only on internal power and network availability.

Complete organizational control over both hardware and data represents another significant advantage. Organizations maintain full ownership and management authority over their backup infrastructure, meaning data never leaves their physical custody unless they explicitly choose to replicate it elsewhere. This level of control satisfies stringent data sovereignty requirements and provides peace of mind for

organizations handling extremely sensitive information that cannot be entrusted to third-party cloud providers.

Security

From a security perspective, on-premises appliances offer the option for physical isolation when not actively performing backup operations. Organizations can implement network segmentation strategies that disconnect backup appliances from production networks except during scheduled backup windows, significantly reducing the attack surface available to potential adversaries. This capability approaches true air-gapping while maintaining the convenience of automated, scheduled backup operations.

The vendor-hardened operating systems running on these appliances provide inherently reduced attack surfaces compared to general-purpose operating systems. These purpose-built systems include only the minimal software components necessary for backup operations, eliminating unnecessary services and potential vulnerabilities that exist in standard server operating systems. Vendors continuously monitor for vulnerabilities specific to their platforms and can deliver targeted security updates without the complexity of general-purpose OS patch management.

Predictable Costs

The cost structure of on-premises appliances centers on fixed capital expenditure rather than ongoing operational costs. Organizations make substantial upfront investments depending on capacity requirements but then face relatively predictable costs limited primarily to maintenance contracts and occasional capacity expansions. There are no per-gigabyte monthly fees that scale with data volume, making long-term costs more predictable than cloud-based alternatives.

Drawbacks

High Initial Investment

The financial model for on-premises appliances creates significant barriers to entry. Enterprise-grade appliances suitable for protecting sensitive data in organizations facing advanced threats typically require costly investments. Implementation costs add further expenses for professional services, configuration, and integration with existing systems. Organizations must also provide appropriate facility infrastructure including rack space, electrical power, cooling systems, and physical security measures.

Operational Burden

The operational burden of managing on-premises appliances falls entirely on the organization. Hardware failures require internal response or vendor support engagement, firmware updates need careful planning and testing, and component replacements must be coordinated and executed by qualified personnel. Organizations need dedicated staff members with expertise in both the specific appliance platforms and general backup architecture principles.

Capacity planning becomes a critical responsibility that organizations cannot easily adjust after initial deployment. Unlike cloud storage that scales on demand, physical appliances have fixed capacity determined at purchase time. When storage needs exceed appliance capacity, organizations face expensive "forklift upgrades" requiring purchase and deployment of additional or replacement hardware. Geographic distribution multiplies this challenge, as each location requiring local backup capability needs its own appliance infrastructure.

Scalability operates on procurement and deployment timelines measured in weeks or months rather than the minutes or hours possible with cloud solutions. Organizations must anticipate future needs, navigate vendor negotiations and procurement processes, wait for hardware delivery, and complete installation and configuration before additional capacity becomes available. This slower scaling can create situations where backup capacity constraints limit business operations or force difficult decisions about what data receives protection priority.

Magnetic Tape with WORM Technology

Magnetic tape storage using Linear Tape-Open (LTO) technology with hardware-enforced Write Once, Read Many capabilities represent one of the most mature and proven approaches to immutable backups. These tapes can be used individually in standalone drives or managed at scale through automated tape libraries featuring robotic systems that handle hundreds or thousands of cartridges.

The physical immutability of LTO-WORM technology operates at the tape drive hardware level rather than through software controls. When a tape cartridge is formatted as WORM media, the drive electronics physically prevent any overwritten operations, making it impossible to alter data once written regardless of what commands software attempt to issue. This hardware-enforced protection creates a fundamentally different security model than software-based immutability approaches. The true air gap capability emerges when tapes are ejected from drives and stored in physically separate locations, creating complete disconnection from any network infrastructure that attackers might compromise

Benefits

Easy Air-gapping

Tape backup systems, particularly with modern LTO technologies, provide unmatched air-gapped security that software-based approaches cannot replicate. Once a tape is written and removed from the drive, it exists as a completely standalone artifact with no network connectivity, no operating system vulnerabilities, and no accessible attack surface for remote adversaries. Physical possession of the tape cartridge becomes the only path to access the data, making tape archives immune to network-based ransomware attacks, remote data manipulation, or unauthorized deletion attempts.

The ability to store tapes in physically secure off-site locations adds another layer of protection that addresses both security and disaster recovery concerns. Organizations commonly maintain tape rotation schedules where recent backups remain on-site for quick access while older archives move to geographically distant secure facilities. This geographic distribution protects against regional disasters, facility-level compromises, and scenarios where on-site infrastructure becomes completely unavailable.

Low Cost

Tape storage delivers the lowest cost per terabyte of any immutable backup technology. Unlike cloud storage with recurring monthly fees, tape represents a one-time media purchase that organizations can use for thirty years or more under proper storage conditions. For organizations with long retention requirements, this cost structure becomes increasingly favorable compared to solutions charging ongoing fees.

The absence of recurring cloud subscription costs makes tape particularly attractive for archival use cases where data must be retained for years or decades but rarely needs to be accessed. Organizations pay only for the physical media, the tape drives or libraries to write and read them, and the physical storage facilities to house them. Once written, a tape sitting in a vault incurs essentially zero ongoing costs beyond the minimal facilities expenses.

Drawbacks

Operational Complexities

The operational reality of tape backup involves significant manual processes and logistical coordination. Physical air gap backups typically involve manual transport and storage media management, including tracking which tapes contain which data, maintaining rotation schedules, coordinating transportation to off-site facilities, and managing retrieval when data needs to be restored. This manual handling introduces opportunities for human error including mislabeling, misplacement, or damage during transport.

Recovery operations from tape are substantially slower than disk or cloud alternatives due to the sequential access nature of tape technology. Unlike disk systems that can seek directly to requested data, tape drives must read sequentially through the media, potentially taking hours to locate specific files on a tape containing terabytes of data. Full system restores from tape can require days to complete, making tape unsuitable as the primary recovery mechanism for systems with aggressive recovery time objectives.

Media management complexity scales with the size of tape deployments. Organizations using tape at enterprise scale need comprehensive tracking systems to maintain accurate inventories of thousands of cartridges, document what data each contains, track retention periods, and coordinate movement between on-site and off-site locations. Rotation schedules require careful design to ensure that appropriate recovery points remain accessible while older tapes move through their lifecycle to eventual secure destruction.

Performance and Technical Limitations

The sequential access model of tape creates inherent performance limitations for recovery operations. Tape drives cannot randomly access data locations, meaning they must read through intervening data to reach requested information. This characteristic makes tape particularly unsuitable for scenarios requiring frequent access to specific files or databases. Additionally, a single tape drive cannot serve multiple concurrent restore requests effectively, as it must complete sequential reads for one request before beginning another.

Human error vulnerability represents an often-underestimated risk with tape operations. Manual handling creates opportunities for tapes to be mislabeled, lost, damaged, or inadvertently destroyed. Unlike software-based systems with automated processes and audit trails, tape operations depend heavily on careful human execution of procedures and thorough documentation of actions taken.

Implementation Comparison

Criteria	Cloud	On-Premise	Magnetic Tape
Ransomeware Protection	Excellent	Excellent	Excellent
Recovery Speed	Fast	Very Fast	Slow
Scalability	Excellent	Moderate	Good
Initial Cost	Low	High	Moderate
Ongoing Cost	Moderate – High	Low – Moderate	Low
Management Complexity	Low	Moderate	High
True Air Gap	No	Optional	Yes
Network Dependency	High	None	None
Implementation Time	Days	Weeks	Weeks
Expertise Required	Low	Moderate	Moderate – High
Vendor Lock-in Risk	Moderate	Moderate	Low
Long-term Archival	Good	Good	Excellent

D. Layered Approach for Better Resilience

Modern backup strategies must balance two seemingly competing requirements: the operational need for fast, flexible daily backup and recovery operations, and the security imperative for immutable protection against sophisticated attacks. Gartner's paper "Ransomware Recovery Requires a Layered Recovery Response" addresses this challenge by advocating for a tiered approach that integrates both conventional and immutable backup technologies, each serving distinct operational and security purposes.

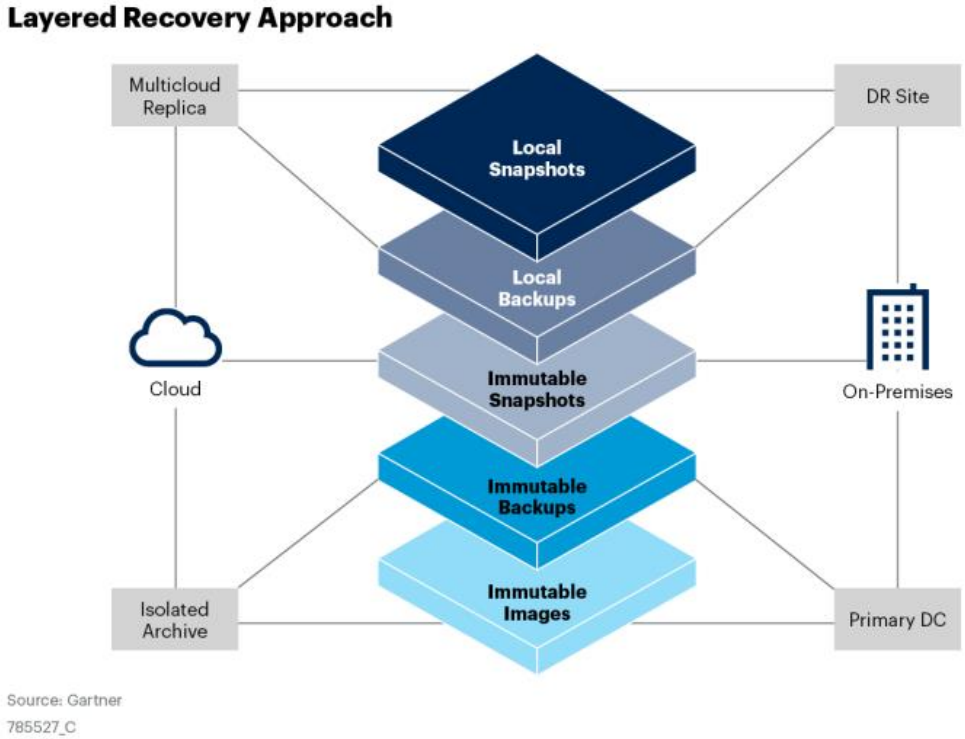

Figure 1 - Gartner - Ransomware Recovery Requires a Layered Recovery Response (March 2025)

It must be recognized that immutable backups, while providing superior security characteristics, introduce operational constraints that make them suboptimal for routine recovery operations. Immutability features that prevent unauthorized deletion or modification also add complexity to normal backup management tasks such as expired backup cleanup and policy adjustments. Additionally, some immutable technologies like air-gapped tape systems involve extended recovery times unsuitable for operational incidents requiring rapid restoration.

A properly architected layered strategy positions immutable backups as the security foundation and disaster recovery backstop, while maintaining parallel conventional backup systems optimized for day-to-day operational recovery needs. This separation of concerns allows organizations to achieve both operational efficiency and security resilience without forcing compromises in either domain.

The usage of immutable backup technologies can be decided by the organization for each layer based on their needs and existing backup strategy. For example, while tape storage is slow, a company that has already implemented this technology can use this for a quarterly backup of their golden images. Allowing to have a strong air-gapped and immutable backup of these crucial resources for a longer time. On the other hand, their snapshots can be stored immutable for a shorter period on their on-premises appliance.

E. What to look for in a backup provider

- **Ensure the provider offers true immutability**
  While a vendor might offer immutability, this is possibly only enforced on software level and can be circumvented if the attacker gains admin privileges on the OS. Make sure that the vendor has hardened the software and hardware so it becomes impossible to circumvent the immutability.

- **Check that the vendor complies with industry standards and government regulations**
  Verify that the provider's solution aligns with recognized cybersecurity frameworks including the CyberFundemantals framework. Or that the vendor has security certifications like ISO 27001 or SOC 2. Verify that the backup solution follows government regulations and that the data is stored in an allowed location, like a European data center.

- **Ensure that the vendor uses strong data encryption at rest and in transit**
  Confirm that the vendor has implemented strong encryption and verify that data in transit is also encrypted to prevent interception during backup operations. Evaluate the vendor's encryption key management practices and if it is possible to use your own encryption keys for enhanced protection.

- **Evaluate the vendors ability to scale**
  Assess whether the solution can accommodate your organization's current data volumes and projected growth over the next three to five years without requiring complete infrastructure replacement.

- **Make sure that the backup solution integrates seamlessly with your infrastructure**
  Verify that the vendor's solution supports all operating systems, virtualization platforms, databases, and applications currently deployed in your environment. Confirm compatibility with your existing backup software if you plan to integrate the immutable storage as a repository rather than replacing your entire backup architecture.

- **Assess the providers customers support quality and the details of their SLAs**
  Review service level agreements carefully to understand guaranteed uptime percentages, response times for support incidents based on severity levels, and any penalties or credits if the provider fails to meet commitments. Evaluate the vendor's support availability, whether they offer 24/7/365 coverage or only business hours support. Additionally, consider the vendor's approach to immutable backups and how it aligns with their patching posture. A provider that enforces strong patching processes and uses immutable backups ensures that even in the event of a security lapse or attack, data can be recovered without compromise, offering enhanced reliability and resilience.

- **Choose a provider with a transparent and predictable pricing model**
  Ensure you fully understand all cost components including initial setup fees, ongoing subscription or license costs, storage capacity charges, data transfer or egress fees, and any additional charges for support or professional services. Request detailed pricing scenarios based on your current data volumes and projected growth to avoid unexpected cost increases as your environment scales.

F. Sources

1. Veeam Blog - Immutable Backups & Their Role in Cyber Resilience (February 2025)
   https://www.veeam.com/blog/immutable-backup.html
2. Commvault – Immutable Backup
   https://www.commvault.com/explore/immutable-backup
3. N2W Software Blog - Immutable Backups: How It Works, Pro/Cons and Best Practices (July 2024)
   https://n2ws.com/blog/immutable-backups-how-it-works-pros-cons-and-best-practices

4. State Tech Magazine - Immutable Backups: How They Work and Why State and Local Agencies Need Them (January 2025) https://statetechmagazine.com/article/2025/01/immutable-backups-how-they-work-perfcon
5. Gartner - Ransomware Recovery Requires a Layered Recovery Response (March 2025)
6. Gartner - Critical Capabilities for Backup and Data Protection Platforms (July 2025)