Acronis

WHITE PAPER

Immutable backup

Table of contents

Executive summary

This white paper provides an in-depth overview of immutable backup and its benefits. It highlights the best practices for implementing immutable backup and discusses the differences between it and traditional backup solutions. We then further explore the potential areas of innovation and growth for the technology.

This white paper is a mustread for IT professionals, data backup and recovery specialists, and businesses looking to enhance their data protection measures. We discuss how you can integrate these solutions into your IT infrastructure to build a robust and reliable data backup system, providing the peace of mind that is essential in today's world of ever-increasing cyberthreats.

Introduction

The evolution of the modern technological landscape is underpinned by an incalculably huge amount of data, which must be protected from loss, corruption, and unauthorized access. Although traditional backup solutions have been effective in this regard, the fact that data loss incidents are still commonplace and cyberattacks are increasingly sophisticated necessitates a shift in the backup model. Immutable backup builds on the shortfalls of traditional backup, delivering tamper-proof, ever-evolving techniques that match conventional data protection needs.

What is immutable backup?

The data stored in an immutable backup solution is tamper-proof; this means it cannot be modified, deleted, or overwritten. In immutable backup, data is stored in a read-only format, prohibiting write privileges to ensure data cannot be changed.

Immutable backups can be replicated across various storage media and keep multiple data copies for auditing and version control. They can also utilize advanced security mechanisms such as encryption and multi-factor authentication to offer incredibly secure data protection

Why is immutable backup important?

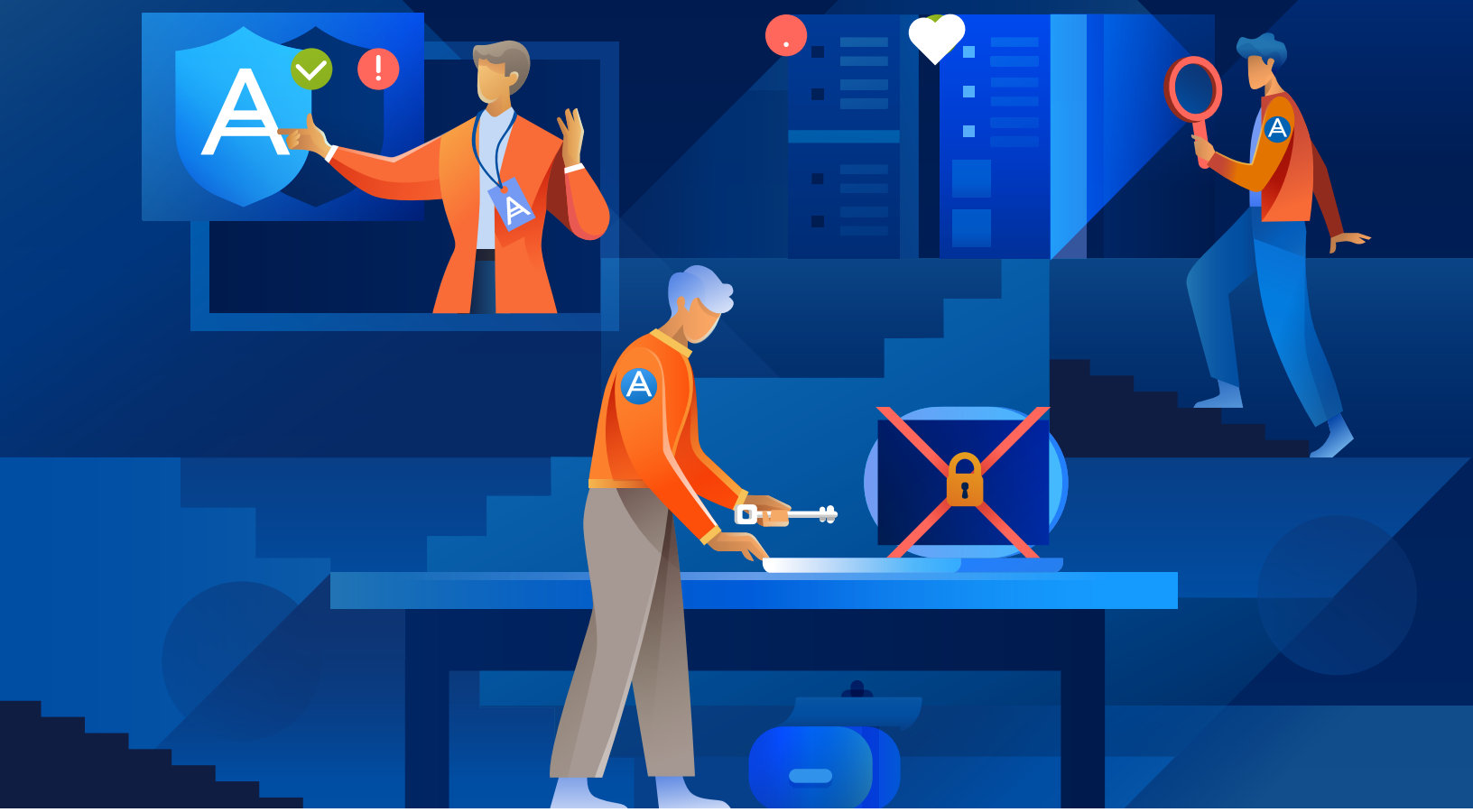
Since cyberattacks and data breaches have become a continuous threat to businesses and individuals, reliable backup is more important than ever. Here are five reasons why.

Data protection

Data loss results from many causes, such as human error, hardware failure, software glitches, and accidental deletion. However, they all have one thing in common — backed-up data has been modified and tampered with. For example, in ransomware, backed-up data is overwritten and held hostage by cybercriminals. Immutable backup prevents such scenarios by saving a version that cannot be altered, deleted or overwritten, regardless of the circumstance or threat actor; this allows you to recover your data without paying a ransom.

Compliance

Regulations such as the GDPR, HIPAA, and PCI DSS require companies to maintain an immutable copy of their data. Immutable backup provides a reliable way for organizations to achieve regulatory compliance, reduce the risk of penalties and fines, and build trust with customers and industry partners.



Preservation of data history

Having an unchangeable copy of your data enables you to track the evolution of your data over time. This can be particularly useful in legal cases, where evidence of data authenticity and integrity is critical. Immutable backups can provide an audit trail that shows who accessed the data, when the data was accessed, and whether any changes were made.

How does immutable backup work

Immutable backup solutions create a read-only copy of the data, ensuring no one is able to modify or overwrite it. This is achieved by way of encryption, whereby users must be authorized and authenticated to access the data. Immutable data is also stored in a compressed format to reduce storage requirements and provide faster restores.

There is a growing application of the nonfungibility of blockchain technology in immutable backup solutions. With this, every event, such as the creation of a backup or restoration from a backup, can be stored in a "block" that is connected cryptographically to a well-defined, sequential arrangement of blocks. This improves data authenticity — especially for in-house data recovery specialists.

Immutable backup solutions also provide a chain-of-custody tracking solution by registering every data transaction and creating an audit trail that can help identify the source of any unauthorized change or breach. This provides an additional security layer against cybercriminals.

Immutable backup solutions

There are five types of immutable backup that are the most widely used today.

Write once, read many (WORM)

WORM backup is an immutable backup solution that creates a non-erasable copy of your data. The data is written to the backup disk, such as a CD, DVD, or magnetic tape, once, after which it is read-only. WORM is mostly used for long-term archiving of sensitive data, such as medical, financial, legal and regulatory records.

Continuous data protection (CDP)

CDP backs up data continuously and consistently, providing a granular restoration of data changes at

any time. Changes made to the data in the primary storage are automatically copied to the backup storage, ensuring the data is always available in the most recent state. CDP backup solutions back up data at intervals of seconds or minutes.

Time-based snapshots

Time-based snapshots are taken at specific intervals using a delta algorithm. Each snapshot includes only the changes that occurred since the last backup. Time-based snapshots are ideal for storage systems shared by many virtual machines. Snapshots are taken frequently to facilitate data restoration, with a recent snapshot always at your fingertips.

Versioned backups

A versioned backup solution enables the creation of multiple versions of the same data. The backups preserve each copy of the data, ensuring that previous versions are available and recoverable at any time. The data versions provide an audit trail of changes to the data, enabling businesses and corporations to compare and restore the previous version, should it become necessary. Versioned backup solutions are typically used for critical business data, such as financial records, source code and software projects, where files are updated frequently.

Cloud storage-based immutable backup

This immutable backup solution employs remote cloud servers to store backups, guaranteeing that the data is accessible from anywhere. Organizations can also scale cloud backups up and down as their data storage requirements change. Most cloud immutable backups offer a pay-as-you-go pricing model and robust security features such as encryption and multifactor authentication.

Immutable backup vs. traditional backup

The differences between immutable and traditional backup solutions are significant, as discussed below.

WORM technology

Immutable backup solutions implement WORM technology to protect data from modification or deletion. This ensures that data written to the backup media can only be read, and not overwritten — making it permanent and tamper proof. On the other hand, traditional backup solutions use media that can be overwritten, making them susceptible to accidental or malicious modification or deletion.

Note: It can be more expensive and complicated to set up and maintain WORM technology compared to traditional backup solutions.

Data retention

Immutable backup offers a higher level of data retention, while traditional backup solutions have a limited retention period. Although this is an advantage, it becomes disadvantageous when nonimportant, unnecessary data are retained long term.

Security

Thanks to WORM technology, immutable backup offers higher security than traditional tools. This is especially important considering data integrity, which is critical for sensitive data like financial records or other highly confidential information. Immutable backup solutions also detect data breaches faster and provide quicker remediation.

Cost

Compared to traditional backup solutions, immutable backup solutions can be more expensive to implement because they require specialized hardware and software.

Flexibility

Regarding control over backup scheduling, traditional backup solutions are more flexible since you can customize the backup frequency. Immutable backups are, on the other hand, automatic, meaning you have far less control.

Reliability

Immutable backups are more reliable than traditional backups. Because the former cannot be modified or deleted, they provide a more robust level of protection against data loss or corruption.

Cloud-based immutable backup solutions

In today's cloud-first world, cloud-based immutable backup tools are essential. They offer reliable, secure and tamper-proof backups. Cloud service providers also have the expertise and resources to provide customers

with advanced security measures including encryption and access controls. This means that data backed up to the cloud is generally considered better protected than on premises.

Cloud-based immutable backup solutions also eliminate the need for IT teams to purchase and install hardware and software, enabling them to seamlessly scale their backup requirements as data volumes grow. They are easier to oversee as well. The cloud provider manages the hardware, infrastructure and software required for backup — meaning IT professionals, data backup and recovery specialists and business organizations do not have to handle any backup infrastructure.

In addition, cloud-based immutable backup tools offer a higher level of accessibility. Since backups are stored in the cloud, they can be accessed from anywhere. This ensures that data is accessible to authorized users, irrespective of location, increasing productivity and efficiency in a distributed workforce.

Best practices for immutable backup implementation

If you are considering implementing an immutable backup solution for your firm or organization, there are some best practices you should adopt.

Establish a backup and recovery plan

The plan should outline the procedures to be followed in the data backup and restoration process. It should also specify the frequency and types of backup to be performed. The backup plan should be well documented and communicated to all stakeholders.

Choose the right hardware and software

The hardware and software for your immutable backup should be reliable, secure, and compatible with your system. Determine your required features, such as encryption, compression and remote backup management. Choose software that allows you to automate the backup process, monitor backups and receive alerts when errors occur.

Implement access controls

While immutable backups are resilient data protection solutions, it is important to also ensure only authorized users have access to the data. Strong passwords and multifactor authentication are required to achieve this, as well as audit logs for all backups and restorations; make sure to review the latter regularly for any suspicious activities.

Encrypt data

Encryption is a crucial security measure that guarantees access to your backups is limited to only those with the proper credentials. When setting up immutable backup solutions, make sure data is encrypted in transit and at rest.

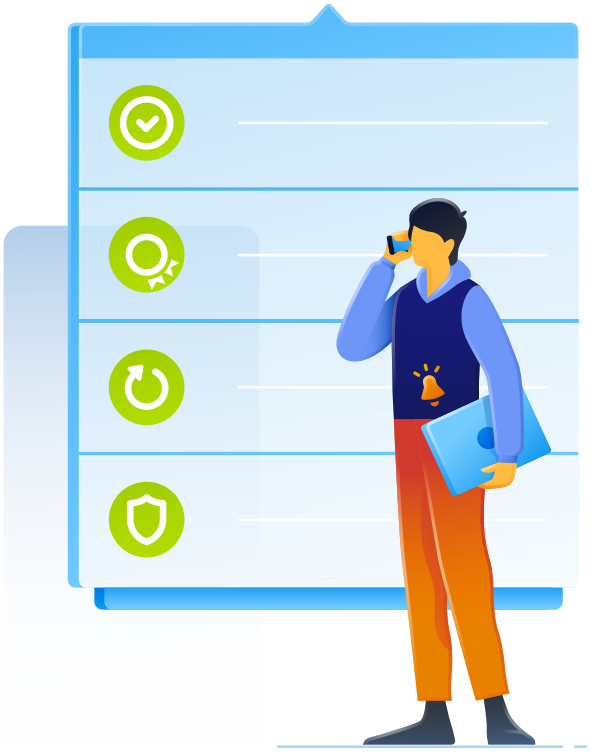
Powerful encryption algorithms, such as the Advanced Encryption Standard (AES), are a critical factor in ensuring data cannot be easily decrypted. Moreover, you must also ensure that the encryption keys are stored securely and that only authorized users have access to them.

Implement monitoring

Monitoring helps you keep track of the backup process and detect any issues before they become significant. Implementing monitoring involves setting up alerts and notifications that will inform you when backup and restore operations are complete, unsuccessful or require attention. Monitoring also includes analyzing historical data to identify trends and make informed decisions about future backup operations.

Test your backup and restore procedures

Backing up data is just one part of the process; the other critical part is restoring the data in case of a disaster. Testing your backup and restore procedures regularly is essential to ensuring that your backups can be restored when needed. This includes performing a complete system restoration using both partial and complete backups to see if your backup solution will deliver the desired results. Moreover, you should test your backups under various scenarios, such as accidental deletion of data, hardware failures, or cyberattacks.



Implement an off-site backup solution

Business and corporate organizations must implement an off-site backup solution to protect their data from physical loss. Storing backed-up data in another location protects it against natural disasters, including fires, floods and other events at the primary location. When implementing an off-site backup solution, you must ensure that the backup infrastructure in the off-site location is as secure and reliable as the primary location. Also, establish a communications plan to inform the backup location of any data changes so that they remain up to date with the latest data backups.

Train your staff

An organization's personnel must know how to effectively use the immutable backup tool. Training should cover all types of backups performed, how frequently the backups must be made, how to access the data backups when needed, and how to restore data in case of a disaster. Staff must also understand best practices for handling sensitive data and the importance of keeping backups safe and secure. Knowledge about anti-money laundering (AML) compliance and other relevant regulatory requirements is key.

The future of immutable backup

Immutable backup solutions are becoming increasingly popular and the future looks ripe with significant innovations and growth in terms of their efficiency. Here are some current forecasts.

Integration of artificial intelligence (AI) and machine learning (ML)

These technologies are advancing quickly and can be used to analyze data backup trends, optimize backup schedules, and improve the speed of backup and recovery. AI can also detect and deter data breaches, providing more advanced threat detection and mitigation.

Greater adoption of cloud-based Solutions

The adoption of cloud-based immutable backup solutions will likely continue to grow, as they offer scalable and flexible storage that can accommodate

data growth without additional infrastructure. They also offer the advantages of quick disaster recovery, easy scalability, and the ability to access backups from anywhere with an internet connection.

Increased focus on compliance and regulatory requirements

As data privacy and security continue to evolve and become more mainstream, there will be greater demand for immutable backup solutions that comply with regional and international regulations such as GDPR, HIPAA, and PCI DSS.

Higher priority for data governance

Organizations will pay greater attention to data governance in the face of increased data volume and complexity. Immutable backup solutions must work closely with compliance and legal teams, providing improved data management and access controls. Advances in technology will enable backups to be more searchable and organized, enabling businesses to better protect their data.

Conclusion

Businesses that invest early in immutable backup solutions will reap significant benefits and stay ahead of the competition. The ROI of implementing immutable backup solutions outweighs the complexity it presents.

Acronis Cyber Protect functions like an immutable backup solution with its advanced security features, easy-to-use interface, and innovative approach to cyber and data backup and protection. Learn more about Acronis Cyber Protect today!

About Acronis

Acronis unifies data protection and cybersecurity to deliver integrated, automated cyber protection that solves the safety, accessibility, privacy, authenticity, and security (SAPAS) challenges of the modern digital world. With flexible deployment models that fit the demands of service providers and IT professionals, Acronis provides superior cyber protection for data, applications, and systems with innovative next-generation antivirus, backup, disaster recovery, and endpoint protection management solutions powered by AI.

Founded in Singapore and headquartered in Switzerland, Acronis now has over 2,000 employees and offices in 34 locations worldwide. Learn more at acronis.com.

Acronis

Learn more at
www.acronis.com