WHITE PAPER | IMMUTABLE STORAGE

Not fit for purpose?
How to store your data truly immutable

RNT Rausch. Making IT possible.

RNT RAUSCH

Not fit for purpose?

How to store your data truly immutable

Immutable storage is the last line of defence against ransomware attacks and other cyber threats. Therefore, it's a must have in your data protection arsenal and one important element in your overall cyber protection strategy. Immutable storage is invaluable for backing up, archiving, and protecting valuable data. This is particularly true for all industries that are dealing with uber sensitive data because they have to meet strict data protection guidelines that even go well beyond legal requirements.

The market currently offers a variety of different technical approaches for immutable storage. However, data is not always stored in a truly immutable way. As long as individuals with full admin rights can still access, edit, delete, or even encrypt data (whether that's intenional or not), the immutability label is only a marketing term. A deeper look at the technical details behind the smart marketing messages unveils the truth and tells if a particular product is fit for purpose. In our digital age with all the rapidly advancing technical evolutions, immutable storage is no longer just immutable storage.

The threat level is higher than ever before

The cyber security report "ENISA Threat Landscape 2023" (ETL 2023) provided by the European Union Agency For Cybersecurity (ENISA) from October 2023 is an annual report on the cybersecurity threat landscape. Like the ETL 2022 report, the current one clearly identifies ransomware attacks, as well as those denial-of-service (DoS) attacks that target the availability of network components and even cause entire systems to collapse, as the greatest threats to the European economy. Due to the current geopolitical situation and the increasing professionalisation of the hacker scene, the threat level is higher than ever before. At the same time, cyberattacks are also causing more business and economic damage in our digitalised world. Here are two examples from the ETL 2023 report:

- Machine learning and Artificial Intelligence models are at the heart of many digitalisation projects and are heavily targeted by cybercriminals.
- Distributed DoS (DDoS) attacks on IoT (Internet of Things) networks are also becoming more frequent and block monitoring systems or manufacturing processes.

The best way to protect businesses of all sizes against all the cyber threats is a strategic end-to-end security concept. Unfortunately, even the smartest strategy cannot guarantee complete protection, only one small security hole let's an attack get past the defences. For example, hackers can still use phishing and supply chain attacks or other social engineering methods to gain access to a company's IT network and encrypt data through a ransomware attack.

A security framework with immutable storage is therefore the last line of defence. When valuable company data is properly stored on WORM storage media (Write Once, Read Many) it cannot be changed, deleted or encrypted. Typical WORM media include optical storage media such as CD-Rs, DVDs, special tape storage technologies or hard disk storage with a software-based lock to prevent files from being modified, encrypted or deleted. After a successful ransomware attack, the IT team can use this unalterable backup to restore all systems quite quickly and lossless from known clean data. Claims for ransom lose the terror and make ransom payments obsolete.

Foto: ©SergeyNivens | Dapositphotos.com

The biggest cyberthreats inside the EU

Ransomware:
Although an estimated 60% of organisations affected by ransomware have paid high ransom demands, in some cases they still didn't gain full access to all their data.

Malware:
In 2022, there were 66 disclosures of zero-day vulnerabilities (software weak points) that had not yet been patched and served as gateways for hackers until they were fixed (zero day).

Social Engineering:
Phishing (sending fake emails by impersonating someone else) is still a popular technique and exists in different variations: targeted spear phishing via email, whaling at executives, smishing via messenger or vishing via phone call.

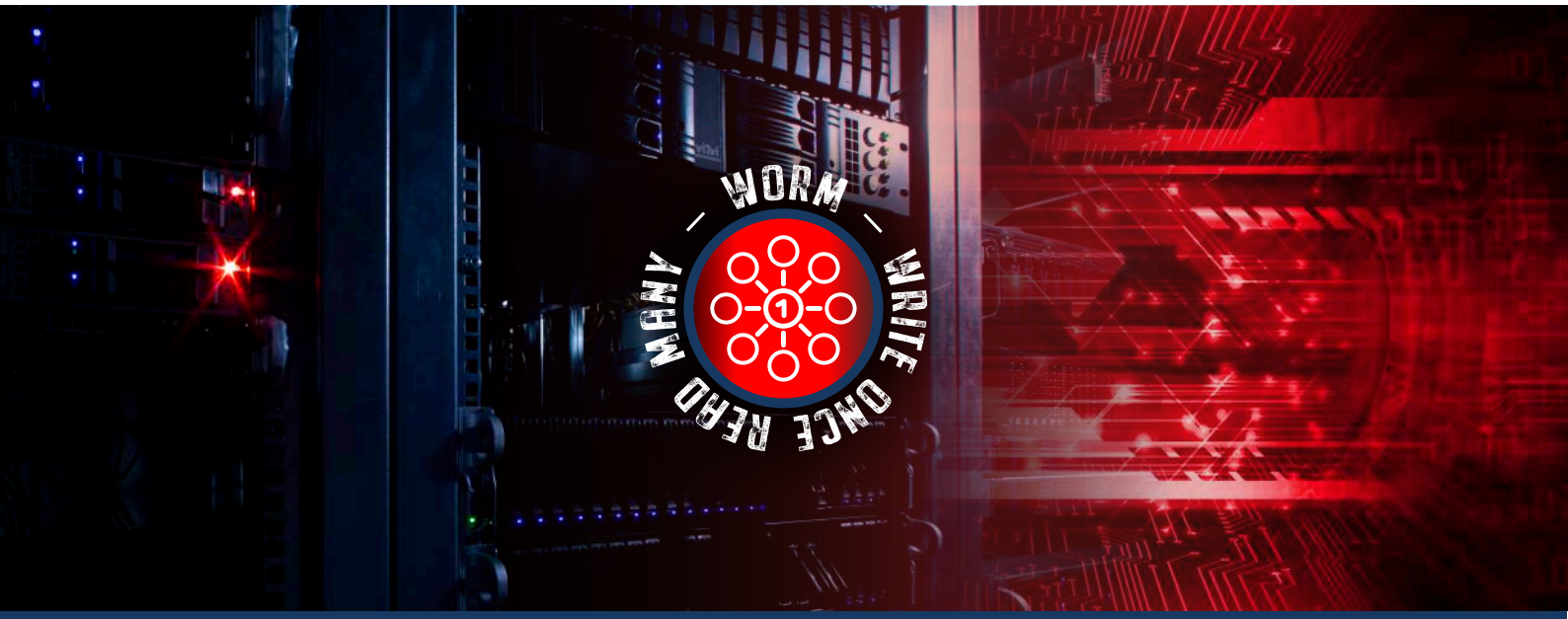
Data attacks
These increase proportionally to the total amount of data produced.

Attacks that threaten IT availability
DoS and DDoS attacks pose one of the greatest threats. The availability of the internet is at risk by the destruction of infrastructure, or massive disruptions and diversions of internet traffic.

Disinformation/Misinformation
Mainly media and social media platforms are a preferred target for AI-based disinformation through deepfakes (manipulation of facial appearance through deep generative methods resulting in deceptively real-looking yet manipulated photo, audio or video recordings) and Disinformation-as-a-Service (false information deliberately spread to deceive people).

Supply chain attacks
Another attack variant on the rise. Cybercriminals penetrate a company's supply chain or network via third-party providers or vendors. In the reporting period, 17% of intrusions were due to supply chain attacks, compared to less than 1% in the previous year.

Source: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023



Immutable storage
to protect valuable data

Technically, immutable storage prevents the encryption, deletion and manipulation of data not only from the outside, but also accidental or deliberate manipulation from within the network, i.e. by human errors or rogue employees.

Until just a few years ago, data storage was immutable according to the traditional WORM standard on compliant media. However, in the age of digital transformation this approach is getting too expensive and inflexible. This due to the huge volumes of unstructured data which we are creating and need to retain affordably.

With that in mind, application-based monolithic data silos in rigid hierarchical structures are no longer suitable for a modern digital world and are becoming a thing of the past. Today, data is stored as objects in unstructured data pools on SDS (Software-Defined Storage) systems, both on-premise and in the cloud. Compared to traditional storage architectures comprising of proprietary hardware and software combinations by manufacturer, SDS helps to decouple these dependencies. The hardware is managed and controlled by an independent software layer that determines, among many other things, how and where the data is to be stored. SDS provides greater flexibility, scalability and avoids costly vendor lock-ins.

However, all the important technical evolutions we're facing require a fresh and extended view at the definition of immutable storage because what used to be quite clearly defined in the older days is now becoming a bit blurry. Data immutability in an SDS environment is no longer only happening at the hardware layer.

Let's have a closer look at other options that are currently available:

① Hardware WORM

This is where it all began. The storage hardware works exclusively according to the WORM principle with one write and multiple reads. On the hardware side you'll find mostly optical, write-once media such as CD-Rs or Ultra Density Optical (UDO) media, which have gone out of fashion in the digital age. However, good old tape has often been declared dead but is still alive and a good choice for certain use cases. All the media described above have only a relatively small amount of storage capacity, which is permanently blocked once the data has been written to it. Data records cannot be erased after the retention period, the only remaining option is physical destruction. Furthermore, the write protection can generally be removed by anyone with physical access to the removable media.

② Systemical WORM – Classical Definition

With systemic WORM, controllers, processors or addressing procedures are designed to store data on a medium in an unalterable and non-erasable manner, thus enabling one-time writability. For example, the integrated processor of a USB flash drive can provide the WORM capability.

③ Systemical WORM – Content-Addressed Storage

When dealing with large amounts of fixed data, Content-Addressed Storage (CAS) is an option worth to have a look at. A dedicated hard disk array stores the information as unique objects. Each object is then stored in a specified area of the disk including the corresponding storage location. Any changes in content of an object would create another and thus different storage location. Objects can only be deleted once the retention period has expired.

④ Systemical WORM: Continuous Snapshots

Continuous snapshots protect data against encryption through ransomware in a similar way.

The storage system automatically creates the snapshots at pre-defined intervals and stores each copy as an independent object. At the moment, ransomware can only encrypt active objects. This makes the previous snapshot unassailable and does therefore reduce the maximum data loss to a few seconds. However, whenever data is changed or deleted a new snapshot gets created by the storage system and consumes additional storage capacity.

Continuous Snapshots are a good option for real-time applications, e.g. Internet-of-Things (IoT) or Industry 4.0, but an expensive way to go for all data that hardly ever get changed and must be stored long term.

⑤ Software-defined WORM for Archiving

By definition, software-defined WORM is dedicated software or firmware that creates the 'write once, read many' capability on the storage system by mimicking the attributes that make physical media like hard disks or LTO-tapes WORM compliant. Software-defined WORM uses electronic receipts (hash codes) and synchronises the system time with a verified server time to accomplish that:

- access and writing records are kept so no one can tamper with data
- data is only written onto a device once
- nobody can delete data
- everybody with valid credentials can read data on demand

Files can thus be protected from accidental or intentional change, deletion or encryption either permanently or until the retention period expires. Many archiving solutions in the market use software-defined WORM as it resolves the size problem with physical media in this age of data volume explosion. However, in many cases, anyone with administrator rights can still encrypt, delete, or change the data.

⑥ WORM – compliant Object Storage - S3 Object Lock

All object storage solutions with full S3 capabilities have access to the integrated Object Lock functionality which is becoming the industry standard for object storage immutability - on-premise and in the cloud. Object Lock is ideal for

- ransomware protection
- archiving with legal retention period requirements
- the need to meet any other regulatory requirements

Many backup software vendors already support Object Lock natively. In object storage data is stored as objects which are organised into buckets with shared metadata. In simple terms, Object Lock has different protection modes and prevents data from deletion, overwriting or encryption for either a user defined retention period or indefinitely until the legal hold gets removed. In Compliance Mode even users with root access privileges cannot tamper the data protected by Object Lock.

Court-proof Storage and Archiving of Heterogeneous Data with S3 Object Lock

Object Lock also enables court-proof recordings of forensic video or audio files. Police, military, and fire brigades already use compact object storage appliances with integrated object lock functionality to store video recordings from body cameras or drones for evidence in a court-proof manner. The object lock function prevents subsequent manipulation of these videos. Likewise, think of documents like contracts in notary offices or law firms, testimonies for court or even medical records or examination results in cases of suspected abuse, rape or assault.

Spoilt for Choice

It's not a surprise at all that the immutable storage solutions have strengths and weaknesses.

For example, in large, virtualised environments classical hardware WORM is no longer a viable option from a financial point of view. Archiving with software-defined WORM or some systemical WORM options still allow data encryption via root admin access. Other options are viable for agile applications or ideal for audit-proof archiving methods. Either way, if you're looking for a truly immutable and audit-proof solution you can only rely on classical WORM media or S3 based SDS solutions with Object Lock.

WORM type	Security level	Characteristics
Hardware–based WORM	★★★★★★	offline, low capacity, complex
Systemical WORM	★★★★★★	offline, low capacity, complex
Content-Addressed Storage	★★★☆☆☆	online, object-based, vendor specific, for certain hard drives only, requires secure admin access
Continuous Snapshots	★★★☆☆☆	online, object-based, vendor specific, requires secure admin access, suitable ransomware protection option for agile applications
Software–based WORM	★★★½☆☆	online, security level depending on admin access rights, reasonable data theft protection for archived data
S3–Object–Lock		online, open standard, limitlessly scalable, legally compliant and audit-proof data storage including full ransomware protection against encryption, deletion, and data tampering

Immutable Storage
Pass Audits. Stay GDPR Compliant and Go Beyond Legal Requirements

Besides meeting legal requirements, another huge advantage of immutable storage is audit compliance. This allows companies to store important files like contracts or financial documents in a way that any kind of manipulation or alteration is impossible. In Germany, this must be done in such a way that the legal requirements with regard to regularity, completeness, security, availability, traceability, immutability and access protection are met.

The General Data Protection Regulation (GDPR) also prescribes the granular definition of access rights to personal data in order to protect it from unauthorised access, data misuse or loss.

Conclusion:
There's No Such Thing as 100% Security

With the exception of hardware-based WORM all options described in the table on page 10 are software-based and therefore never one hundred percent secure. This even applies to S3 Object Lock. Security vulnerabilities in software and hardware can bypass any overwrite protection. For example, if you're operating an agile SDS solution, you simply cannot store the huge amounts of data on CD-Rs. Secondly, anyone who's working with immutable storage must be aware that any backdoor to change the read-only attribute bears the risk that hackers who gained admin rights can use that backdoor to manipulate the data.
This is why every cyber security concept must include stringent measures, such as a zero-trust approach and multi-factor authentication, which are equally and without exceptions applicable to all employees within a company.

In the age of digital transformation and resulting rapid technical evolution, modern and future-proof solutions are designed to offer far more than the highest possible level of data protection. Particularly in hybrid environments, IT decision-makers are well advised that the optimal solution is also compliant with all relevant regulations and legal requirements, especially but not limited to the cloud and cloud-based services. Besides GDPR, or upcoming EU directives like NIS2 or ViDA (VAT in the digital age), this also includes the principles for the proper bookkeeping and associated retention periods. In an international business environment, the requirements of the US supervisory authority SEC or the Swiss FinSA are becoming relevant. Additionally, there are industry-specific guidelines, e.g. for vertical markets and sectors like healthcare, chemicals, pharmaceuticals, finance, education, or automotive.

If you're interested in further information about our immutable storage solutions, please click here.

About RNT Rausch

RNT Rausch is a German based technology pioneer with 25 years of experience in the high-tech server and storage industry. RNT is on a mission to always be ahead of technology trends and specialises in designing future-proof server and storage solutions that go hybrid and tackle your business challenges. RNT makes businesses of all sizes, data centres and service providers fit for tomorrow's technical revolution. RNT's personalised solutions and tailored services let all customers exceed digital transformation goals while optimising security, flexibility, scalability, and sustainability.

Out of Ettlingen, Germany, a passionate team of over 30 experts delivers powerful and intelligent high-quality solutions built to your business needs. We are making IT possible.

For more information,

please visit https://rnt.de/en/

RNT Rausch. Making IT possible.

RNT Rausch GmbH
Im Stöck 4a | 76275 Ettlingen | Germany

Phone: +49 7243 5929-0 | Fax +49 7243 5929-14
Mail: info@rnt.de | https://rnt.de