DCIG

Executive White Paper

The Role of Immutable Storage in Ransomware Protection and Recovery

by DCIG Analysts Todd Dorsey and Jerome Wendt

NASUNI

COMPANY

Nasuni Corporation
One Marina Park Drive
6th Floor
Boston, MA 02210
(857) 444-8500

www.nasuni.com

INDUSTRY

Data Storage

SOLUTION

Nasuni

BENEFITS

- Cloud-native Global File System
- Rapid Recovery
- Reduced Storage Required at the Edge

BUSINESS USE CASES

- Enterprise NAS
- Backup
- Disaster Recovery
- Business Continuity
- Multi-location access (ROBO)
- Distributed workforce (SOHO)

An Unpleasant Truth

All organizations need to face an unpleasant truth: It is not a question of "If" they will experience a ransomware attack; it is a matter of "When." While cybersecurity software serves as a first-line defense against ransomware, some attacks unfortunately succeed. In those instances, enterprises may use immutable storage solutions to protect their data.

An Ounce of Prevention

Statista, a global research firm, reports 304 million attacks worldwide in 2020,[1] or about 800,000 attacks daily. Posts on Quora estimates that the world contains about 300 million companies.[2] This approximate 1:1 ratio of companies to attacks means any internet-connected organization may expect an attack at any time.

To defeat these attacks, the adage 'an ounce of protection is worth a pound of cure' applies. Cybersecurity software continues to represent the first and best line of defense organizations should embrace to block ransomware attacks. It is far better to stop an attack than try to recover from one.

However, IT leaders recognize cybersecurity software alone does not thwart all ransomware attacks. As a result, organizations must assume some attacks will succeed. To prevent an attack from becoming a catastrophe, businesses must protect their production and backup data.

Immutable Storage Solutions

To stop ransomware from encrypting data, administrators may use immutable storage solutions. Storing production and backup data on these solutions provides a viable means of securing data from attacks.

Multiple immutable storage options now exist from cloud storage and networked storage providers. Once files or data is stored in an immutable state, even ransomware cannot alter the data. These solutions protect data from the attack and provide a source to quickly recover data in an unencrypted format.

Cloud Storage for Immutable Storage

Using cloud storage to store backup and production data appeals to organizations now more than ever. Many cloud storage offerings include data immutability features that deliver in one or both of the following two ways:

- ***Journaling or versioning file systems.*** When existing data stored in the cloud gets changed or modified, the cloud does not delete the old version; rather, the cloud versioned file system retains the existing, as well as previous versions of the data as immutable objects. Ransomware may change the visible or current production data; however, ransomware cannot encrypt previously existing data stored in immutable form. Organizations may select a prior, existing version of data and use that version to recover. Some solutions write all files as immutable objects, simplifying the management and recovery of ransomware encrypted data.

Ransomware 2021

600%	Increase in malicious emails since COVID-19[4]
$170,404	Average mid-sized corporation payout[5]
$1.85M	Average organizational cost to recover[5]
21 Days	Average company downtime from a ransomware attack[6]

The largest cost—**Business interruption**[6]

- ***Object Lock.*** AWS introduced S3 Object Lock in 2018,[3] an S3 feature other cloud providers have since released. Object Lock operates like write once, read many (WORM), a technology many organizations know well. Organizations apply and enforce retention policies on data they store on cloud storage. Once data gets written, nothing may change or delete the data until the data's retention period expires.

These two features set cloud storage as a logical option to protect organizational data from a ransomware attack.

Organizations may obtain cloud storage from multiple, general-purpose and purpose-built cloud providers. Any of these options offer cloud storage's lower costs (when compared to production storage), ease of scaling, and storing data off-premises.

The latest backup software and enterprise storage solutions further simplify cloud storage's adoption and use. To use cloud storage, these solutions support the simple storage service (S3) API. These solutions use S3 to interface with the cloud to manage data placement and assign retention policies to the data.

“Organizations should not automatically equate a solution’s support of cloud storage with protection from ransomware.”

Organizations should not automatically equate a solution’s support of cloud storage with protection from ransomware. These solutions must support automatic, or at a minimum, turning on immutable versioning or setting the object lock on the data placed in the cloud. If the solution supports versioning, enterprises should also verify it offers an option to select past points in time for recovery.

Networked Storage with Secure Object Data Stores

Cloud storage has become simpler to implement and use in recent years. And more on-premise storage solutions offer immutable data, cloud storage options. These storage systems provide a standard file system interface that supports the NFS and SMB networked file protocols. In this way, organizations may deploy and access data on these systems like any networked storage solution.

Beneath their file system presentation layer, these storage solutions use an immutable object store. Applications, clients, and users only see and write data to their file system. Once written, the solution automatically stores the data on its underlying object store as immutable objects.

Using this approach, applications, clients and users may still change or delete data presented through the solution’s file system interface. However, the solution’s underlying object store neither changes nor deletes the prior version of the data.

Instead, the storage system’s object store journals all changes. The system chronicles new writes as well as any changes, additions, or deletions of existing data. This technique safely preserves new data as well as the prior, original version of the data. By preserving this data, should a ransomware attack occur, organizations may roll back to a prior point in time.

Immutable Storage—A Critical Role in Ransomware Attack Responses

In summary, every organization should use available cybersecurity software as the first and best line of defense against ransomware attacks. Detecting and stopping ransomware attacks still serves organizations better than recovering from an attack. However, cybersecurity software does not provide a foolproof defense against these attacks.

This data gap dictates that organizations have a recovery plan in place. Placing data on an immutable storage solution plays a critical role in recovering from a ransomware attack. When stored as immutable objects, all data is preserved in an unaltered state, providing organizations with multiple, viable recovery points.

Used in conjunction with cybersecurity software, these immutability features help ensure organizations have the appropriate defenses in place to protect them from the disruption and costs of a successful ransomware attack. ■

1. https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/. Referenced 8/10/2021.
2. https://www.quora.com/How-many-companies-exist-in-the-world. Referenced 8/10/2021.
3. https://aws.amazon.com/about-aws/whats-new/2018/11/s3-object-lock/
4. https://abcnews.go.com/Health/wireStory/latest-india-reports-largest-single-day-virus-spike-70826542 Referenced 8/12/2021
5. https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf?cmp=120469 Referenced 8/12/2021
6. https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020 Referenced 8/12/2021

About DCIG

The Data Center Intelligence Group (DCIG) empowers the IT industry with actionable analysis. DCIG analysts provide informed third-party analysis of various cloud, data protection, and data storage technologies. DCIG independently develops licensed content in the form of TOP 5 Reports and Solution Profiles. More information is available at **www.dcig.com.**

DCIG, LLC // 7511 MADISON STREET // OMAHA NE 68127 // 844.324.4552