Protecting Data

Data is always at risk of loss or corruption, whether it's from ransomware encryption, viruses, trojan horses, hardware failures, or human errors. A ransomware attack is particularly damaging because it can quickly encrypt a large amount of data and suddenly stop all system activity unless a ransom is paid. The time it takes to recover a system and how much data we might lose in the process are critical factors in most decisions about whether or not to pay the ransom. How fast and how well a solution can recover a system and its data makes a huge difference between paying a ransom or recovering from an attack without paying.

> The difference between paying a ransom and recovering a system boils down to how fast and how well we can recover it ourselves.

Traditional Approaches

Typical ransomware recovery solutions rely mainly on backups or snapshots to preserve data at regular intervals. Should an attack occur, we can use those backups and snapshots to restore a system to a known, clean state. Of course, we'll want to take backups and snapshots as frequently as possible to reduce data loss, but the time they take, the amount of storage they consume, and the overhead needed to manage a large number of backups and snapshots invariably force us to compromise.

To protect the backups and snapshots from ransomware, many solutions also store copies on immutable storage so that they are physically unalterable. However, backup systems run on servers and use databases to keep track of backups and snapshots, so these servers and databases must also be protected against accidental loss and ransomware attacks in order to be able to restore from them.

COSNIM Technology

COSNIM takes a very different approach. Instead of relying on traditional snapshots and backup copies that were taken at precise intervals to protect data, COSNIM directly records all updates in a patented protected mesh (called a Continuum) that seamlessly tracks all changes and allows users to easily go back in time and examine absolutely any data, at any past point in time, instantly. Time-Travel protection incurs no additional overhead, and all historical information is immediately and transparently accessible through the filesystem as easily as browsing directories.

> COSNIM Time-Travel is zero overhead, always-on protection, with instant access to all past data.

As Time-Travel runs continuously, it provides extremely high-frequency data protection without the overhead and costs associated with traditional backups and snapshots. As COSNIM also operates without the use of servers or databases, there is no additional infrastructure to protect against loss or ransomware attacks in order to recover from it.

Instant Immutability

COSNIM packages all data, metadata, and control information entirely in storage capsules. These capsules can be stored directly in immutable storage without any intermediary processing. This means that all data stored in COSNIM is instantly protected against ransomware as soon as it is produced and stored – no waiting for backups, extra copies, tracking or subsequent processing by a server.

Low RPO

Time-Travel protection is continuous and instantly protects the most minute changes to data. When COSNIM is used for live storage, data is immediately protected by Time-Travel as soon as it's updated and stored, without the overhead, costs, or delays of traditional backups and snapshots. When COSNIM is used instead to perform backups of another filesystem, all backup points (in fact, everything that's going on *during* backups) are also continuously protected by Time-Travel, transparently.

> Time-Travel continuous data protection greatly improves the precision and quality of the recovered data.

Since Time-Travel has zero processing overhead, extremely low storage overhead, and does not require the use of any databases or servers, it can protect data at an extremely high rate and track a large number of recovery points without the limitations of traditional backup and snapshot solutions. This makes it possible to have extremely low Recovery Point Objectives (RPO), down to fractions of a second, which greatly improves the precision and quality of the data that's available to recover a system.

Instant Ransomware Recovery

Ransomware encryption attacks usually start stealthily, gradually encrypting data in the background until the ransomware decides to make its presence known. This means that recent backups and snapshots that were taken may also contain some ransomware-encrypted data. During recovery, it's critical to determine when the attack started so we can pick the right backup or snapshot to recover from. With traditional technologies, this discovery can be quite time-consuming, especially if we need to also restore the data to ensure it's in fact not encrypted.

In COSNIM, there's no real difference between backups, snapshots, versioning, archival, and live storage. Everything is equally protected by Time Travel and always securely accessible directly through the filesystem as if it was live data. This means that discovering when an attack started and examining which files were affected is as easy as browsing directories, with immediate access to all past and current data. This greatly increases the speed at which a system can be recovered from a ransomware attack.

Cherry-Picked Recovery

Because ransomware usually targets only a strategic set of files to encrypt and perform encryption gradually, recent backups and snapshots will often contain a mixture of clean and corrupted files or file fragments. With traditional solutions, you'd have to mount or restore each snapshot or backup individually to check and identify which data is good or not, which can be quite time-consuming, especially if you need to restore multiple versions before getting it right.

> Accessing past data is as easy, and as fast, as browsing live data.

With COSNIM Time-Travel, since all past data is accessed directly as a live filesystem, wherever the data is physically stored, you're free to examine multiple Time-Travel points simultaneously, and easily cherry-pick the right files to recover directly from the filesystem, without delay. You can also easily compare different versions of a file to make sure you're making the right choice, without waiting for restores. This makes it possible to quickly identify and restore the best version of data with extreme precision.

Continuous Protection, Even During Recovery

Suffering and recovering from a ransomware attack with COSNIM doesn't mean you stop being protected. In fact, even during an attack and while recovering from it, COSNIM Time-Travel can continuously protect and record data changes, as they occur. With deduplication active, restoring old data on top of corrupted files won't even occupy additional storage space, since COSNIM will quickly identify and reuse the same ransomware-proof immutable storage capsules that were recorded before the attack occurred, saving valuable space.

Forensic Analysis

As COSNIM can continue running and tracking changes while you're being attacked or restoring a system, everything about the attack itself and the recovery is also recorded by Time-Travel. This means you have instant access to all the damaged data for later forensic analysis, without having to take any special backup or copy of the damaged system before starting the recovery. Combined with Time-Travel

audits, you can even analyze precisely, piece by piece, each file or data fragment that was encrypted by ransomware and later restored, all directly from within the filesystem.

Ransomware Indices

Lastly, COSNIM can also compute "ransomware indices" of data as it's updated live to quickly detect and alert you of an attack. These indices measure in real-time the randomness of data as each fragment is updated. If the randomness of data fragments starts increasing abnormally, this can easily signal a ransomware attack, information which can be fed live to a monitoring system or AI for immediate analysis and/or defensive measure.

> With live ransomware analysis and instant audits, COSNIM helps to quickly detect and react to an attack in progress.

Ransomware indices are also recorded directly inside capsules alongside metadata, tracked by Time-Travel, meaning that this information is instantly available from any other system that also has access to the storage capsules, without any access to the system that's producing the data or possibly suffering from an attack. Combined with Time-Travel audits, which identify precisely which data fragments were updated, plus the ability to quickly examine before and after versions of files and data fragments directly through the filesystem, this gives security analysts and automated systems extremely powerful tools to quickly detect, analyze, and recover from ransomware attacks.

Suffering a ransomware attack and trying to recover from one is a painful experience. COSNIM, with its unique capabilities, can help tremendously to better protect yourself and recover from such attacks.

Https://www.cosnim.com
info@cosnim.com
+1 888 212-3527