Chains Explained: Why You Need Chain-Free Backup in Your Data Protection Plan

Why Chain-Free Backup is Awesome

To put it incredibly simply, chain-free backup is a modern solution that eliminates the pain points of chains.

When corruption or malware occurs, bad data blocks are isolated and can be independently deleted without any risk of breaking any kind of data integrity in your backup dataset like traditional chain-based backup technologies. Previous backups can still be recovered almost instantaneously, with new incremental backups being taken as your team creates new work data. There is no data loss and no wasting of time or storage.

Near-Instant Recovery: No chains mean nocomplicated dependencies or processes based on your historical data. This new technology is advantageous because it significantly reduces the complexity of recovery to keep your business running with uninterrupted business continuity.

A Primer on What Chains Have to Do with Backups

Chain-based technology is also referred to as traditional/forward or inverse/reverse chain backups.

Traditional/forward chain is the backup architecture that started it all. To understand chains, we need to start with their role in the backup process.

First, all your data needs to be backed up and then replicated to the cloud so that when disaster strikes, the backups can be restored, ensuring your business continuity. The problem is that this first step of backing up and replicating to the cloud takes a lot of time. So to be efficient, subsequent backups are incremental. This is where things start to differentiate…

Failed Backups and Consolidation Headaches

Some chain-based technology includes alert settings to notify your MSP if backups appear invalid for any reason.

However, sometimes backups can appear normal even after a break in the chain. Imagine discovering a month's worth of hourly backups – hundreds of backups – have failed. Because chain-based backups require consolidated data from older links in the chain to be valid, all of these backups are lost, and the data is unusable.

To solve for this common problem, some chain-based technologies come with 'consolidated daily' or 'consolidated monthly' backups to create fewer links susceptible to breakage. So hourly backup links are reduced from 24 links in the chain down to just one. Some technology can even consolidate a whole year of backups into just one link. The problem with consolidation, however, is it reduces backup granularity. When you consolidate, you lose the ability to restore from an exact point in time, thus increasing downtime and the complexity required to restore your data in the case of an incident.

Compliance Costs, Data Storage and Reseeding

From a compliance standpoint, chain-based backups threaten adherence to HIPAA standards and legal regulations that require multi-year backup retention.

Therefore, chain-based architectures should never go on past 12-24 months. With a 24-month maximum, the sheer quantity of backups to maintain and store is enormous.

To meet industry compliance standards with chain-based backups, your MSP may have to go to each of their clients and start from scratch every year. A tracking system is also necessary for the appliances or storage media holding data. Technicians must go on-site, copy the data, migrate and store it somewhere else, and start the chain from scratch. Obviously, the time, technician expertise, storage resolution, and reseeding add substantial costs to your services.

Legacy Chain Pain Points That Never End

Regardless of the direction of the chain, chain-based backups are considered 'legacy' at this point because the infrastructure is risky, problematic, and jeopardizes BCDR. As most businesses now accept, data loss will occur. It's no longer a question of if but when a data breach will happen, and that's when backups are critical to business survival. It's these challenges that have MSPs breaking the chains of backup:

- **Storage Bloat:** Even consolidated data cannot be deleted unless a specific deletion policy is created and maintained. Due to the needed consolidation functions to keep the number of links (points of failure) in your backup down to a minimum, it is also doubling your storage footprint for the time prior to your retention policies trim your backup data.
- **Compliance:** Many industry-specific standards require multi-year retention, but chain-based technology should never be used without maintenance past 12 to 24 months and requires yearly reseeding.
- **Recovery Speed:** When disaster strikes and you need your backup data, you must consolidate the base image to the time and data date you want to restore, then restore the data from an accessible 'now-readable' file. This long and resource-heavy process puts unnecessary downtime on your client's business, especially when virtualizing cloud data.

40% of attacks require >8 hours to address – typically at a cost of €100-€250/hour. *Chain-Free is the Smart Move.

Contact us to get chain-free backup and near-instant recovery added to your services today.

nuatech

Email: hello@nuatech.uk

*Source: The hidden costs of ransomware. Webroot.