

FALCONSTOR

How Cloud and Ransomware Broke the 3-2-1 Backup Standard

And What's Next in Backup Methodology

Executive Summary

The 3-2-1 Backup Standard served the Information Technology industry well for decades, but the rise of the cloud as a backup tier and the unfortunate increase in ransomware attacks has put this time-tested process in jeopardy. It appears that the need for fast operational recovery in the face of cyber attack is only a matter of time. To maintain system and data health and meet a cyber attack head on, today's backup process has to ensure a high level of recovery speed from any location and tight security across all media and locations with a cost profile that enables IT to deliver without the need to cut corners.

The 3-2-1 Backup Standard

3-2-1 Backup has been the standard in data protection for decades: retain three copies of your data, the original plus two backup copies, each of which should be stored on different media, with one moved off site for safe-keeping. But does it still hold true in a cloud-dominated world? And if not, what should organizations be doing instead? In other words, should we throw out 3-2-1 completely or adjust it to fit the needs of the cloud?

Back in the day, 3-2-1 typically meant that the original copy was retained on a server on premises. The remaining copies consisted of backup tapes – one on site and one stored externally. The 3-2-1 pattern evolved as a way to provide a copy for operational recovery and another for longer-term security and compliance. The longer-term copy was stored offsite to create an air gap so the organization could recover from digital or physical theft. Tape backups were tested to ensure they were complete and that data all could be recovered.

The Evolution Begins

A series of innovations began to challenge this standard. Disk-based backup, disk-based staging of backups, and Virtual Tape Library (VTL) technology began to supplant tape for operational recovery. When disk-based storage volumes exploded, deduplication burst onto the scene. The new “standard” was to buy two deduplication appliances – one as a backup copy and replicate that copy to the other box. This solution certainly had value, but it proved a little clunky. Restores were slow. Surging data volumes filled up appliances. It became expensive to keep adding more boxes. Tapes remained in use in many enterprises as a medium for long-term backup copies due to their price advantage.



But it was the cloud that really upset the equation. The moment data began to migrate offsite onto the cloud, serious cracks appeared in the 3-2-1 arrangement. It became possible to maintain three copies without any being on tape. One onsite, and two in the cloud, either with the same provider or shared between two providers. Alternatively, there could be a private cloud copy and public cloud copy. Such arrangements appear to satisfy most data and security goals.

- Operational Recovery – on-premise, high-performance disk to meet RPOs and RTOs.
- Long-Term Retention Recovery – off-premise in the cloud. This could be an entire replica system (a substitute for having a second data center) or just storing data in the cloud.
- Security – the move to the cloud increases the need for security via AES-256 encryption in-flight and at-rest.
- Reliability – retrieving data from the cloud drives up egress fees. Thus, it is necessary to test backup reliability without having to move data.
- Air-Gap – some consider the cloud to be a kind of air gap in that it requires a new set of credentials.
- Cost – 3-2-1 in the cloud requires data reduction technology to approximate the cost of long-term retention on tape.

A New Standard Emerges

Rather than throwing out the entire 3-2-1 concept, it is evolving to fit the realities of the cloud and the needs of modern data placement. But what that new standard will become remains to be seen.

Cloud providers offer multiple tiers of storage with different costs, performance levels, and features. Some organizations are attempting to use such tiers to satisfy their data protection needs. A hot tier for data that is accessed frequently, a lower tier for infrequently accessed data, and an archive tier for rarely or never accessed data. That may work for some, but it leaves the organization at the hands of one provider and being left with a single point of failure. The use of multiple cloud providers for different tiers is one solution.

More likely, tape will continue to be used for storage of offsite copies. Indeed, the major cloud providers are among the biggest users of tape in their lowest tiers. Tape after all, provides an actual air gap – a physical barrier between the network and the data. This has proven to be an effective deterrent against ransomware attacks which have proven to be more than capable of infiltrating cloud data stores and disk backups. And because tape goes fully offline, the power and cooling costs associated with rotating media go away.

But tape, these days is viewed largely as an archiving solution. And cloud innovation provides other ways to achieve a similar result to the tape air gap. It remains to be seen how long-term backup and archiving duties will be apportioned between the cloud and tape.

Cloud Immutability and Security

With the right technology in place, the cloud can be as secure as tape via features such as AES-256 encryption in flight and in place, and enterprise-class key management. Embedded hashes and checksums also help to fight against data corruption and misuse, as well as periodically check data health and readiness for recovery. Immutability is provided by the erasure coding that is currently used in warm tiers of cloud-based object storage. And Write Once Read Many (WORM) properties can provide an effective barrier against ransomware and other malware. WORM functionality embedded into backup software can be used by administrators when content is passed to the end media, whether that is cloud or on tape.




Similarly, the latest in backup technology, Virtual Tape Library (VTL), replication, deduplication, compression, multi-tenancy, snapshots, SNMP integration with enterprise management platforms, automation, and software-defined storage are among the many technologies shaping the evolution of 3-2-1. All play their part in providing rapid data backup and recovery of production data as well as the data security needed to survive disasters and cybercrime events.

With petabytes of data in play, modern data protection architectures not only need to scale easily, they must be flexible enough to transmit data from on-premise, primary cloud, secondary cloud, and data archive locations. Each must have the appropriate level of performance and resilience needed by the organization. The recovery pace demanded of production data is far different, for example, than what should be expected from archive or infrequently accessed data. Thus, the factors of speed, cost, and security must be correctly balanced.

Future Patterns

Industry pundits continue to argue over the new standard that is to replace the time-worn 3-2-1. While the underlying philosophy underpinning 3-2-1 is sound, a new paradigm must emerge in the future isn't likely to stray too far from its predecessor but incorporates the wide range of options available today. And new technologies may well appear on the scene that bring about further shifts in data protection and security.



Perhaps we will see cloud providers offering a kind of 3-2-1 service. And backup and storage management vendors taking care of how data is moved from one cloud tier or provider to another. Time will tell.

Clearly, then, it will take some time before a consensus is reached upon the best approach for the cloud era. Whatever that approach is going to be, it must provide fulfill the data recovery needs of organizations in terms of speed, cost, and security. And despite two decades of innovation, it is likely that tape will remain part of the picture for many organizations to satisfy compliance and archiving needs. As a new 3-2-1 paradigm takes over, it is essential to have the backup and storage elements in place and that must encompass both cloud and tape.

The Role of FalconStor®

Meanwhile, in the face of massive data growth, the need to reduce the cost of data protection and the increasing rate and severity of cyber attacks, leading organizations are looking for answers. FalconStor played a role in enabling the old 3-2-1 paradigm, bringing disk into the overall mix in the past, and is defining a new one that blends the right mix of cloud, disk and tape to meet any enterprise requirement. FalconStor's [StorSafe®](#) product, for example, enables secure disk-based data backup and archive, driving out costs with deduplication, securing data with embedded AES-256 encryption, enabling secure replication to cloud and secondary data centers, and, when desired, offload to tape for long-term preservation. It delivers increased data security for data centers and public clouds, and provides the fastest recovery from ransomware attacks while driving down costs by up to 90 percent. To learn more, visit www.falconstor.com.