World Backup Day 2025: Protect Your Enterprise's Data with Next Generation Cyber Secure Backup

Eric Herzog

Eric Herzog
Chief Marketing Officer
Infinidat

Biography

Eric Herzog is the Chief Marketing Officer at Infinidat (https://www.infinidat.com). Prior to joining Infinidat, Herzog was Chief Marketing Office and Vice President of Global Storage Channels at IBM Storage Solutions.

His executive leadership experience also includes: CMO and Senior VP of Alliances for all-flash storage provider Violin Memory, and Senior Vice President of Product Management and Product Marketing for EMC's Enterprise & Mid-range Systems Division.

Eric blogs at https://www.infinidat.com/en/blog

Keywords Data infrastructure, Hybrid multi-cloud storage, Cybersecurity, Return on Investment (ROI)
Paper type Opinion

Abstract

It's important for an enterprise to build cyber resilience into secondary storage to protect backup copies of data. For an enterprise, this is crucial – and each year, World Backup Day is the call to action for cybersecurity decision-makers, such as CISOs, is to ensure cyber secure backup, ideally as part of a next-generation data protection framework, explains the author of this article.

Introduction

Next-gen data protection goes beyond traditional backup, restore and disaster recovery. Putting your enterprise's data in an air-tight cyber repository is not the same as the conventional means of moving data to an online repository as a backup file. Traditional backup environments are high-value targets for cyber-attacks.

The type of backup that combats cyberattacks most effectively is not the same backup as the traditional or conventional approaches that many organizations still utilize. Traditional backup products were engineered to primarily provide high ingest rates by utilizing inline deduplication techniques. Yet, they fall short when it is time

to run recovery operations because their recovery times are exceedingly slow for an era when 24x7x365 IT operations are the norm.

With ransomware, malware, and other cyberattacks increasingly targeting secondary storage, it is important to look to cyber resilient storage with next-generation backup capabilities, including cyber detection, as the path to cyber secure backup. It is necessary to rethink the problem and augment your data protection strategies to counter the way cyberattacks work.

Enterprises need a cyber-focused, recovery-first strategy that enables detection and provides near-instantaneous recovery of data in the event of a cyberattack. This kind of strategy is built on the end-result and everything supporting that result. Neither traditional data protection nor modern data protection will get you there.

Instead, cybersecurity features on secondary storage systems have become necessary for enterprises seeking to protect their backups and accelerate cyber recovery. These need to be part of a business' recovery objectives, which are what next-generation data protection and recovery are focused on.

Points to consider

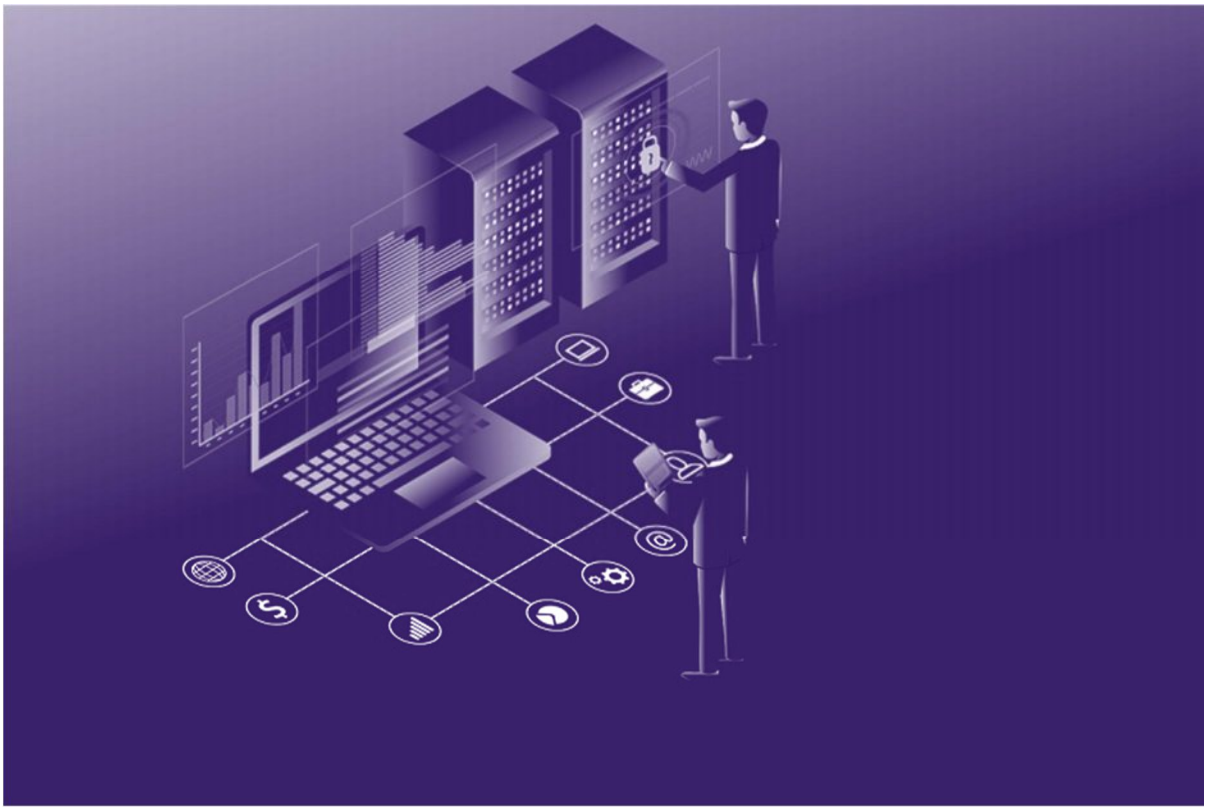
To assess your needs, ask yourself these relevant questions:

- What are the data assets you would need to recover?
- Where do your data assets live?
- How are they being protected today?
- How fast would they need to be recovered?
- How many millions of pounds would your business lose for every minute or hour that goes by without recovering your mission-critical data?
- What other business impact could come from the speed at which you can recover data?
- Do you have business recovery objectives as a central part of your cyber strategy?
- How much risk is your enterprise willing to be exposed to?

Without cyber secure backup, which is rooted in a cyber-focused, recovery-first strategy, enterprises are allowing a dramatically higher level of cyber risk. There is no question that ransomware and malware put your enterprise data at significant risk. The threat is well-understood.

When ransomware takes data "hostage," it can destroy or corrupt backup copies of data. It has caused businesses of all sizes to lose customers, shut down operations overnight, and have their reputations tarnished forever. Furthermore, publicly traded companies must file government documentation on the impact of any cyberattack, and the filing becomes a matter of public record.

So, why would you not deploy cyber secure backup on your secondary storage? Each year World Backup Day is a reminder for businesses to consider the options. But really, the date in the calendar needs to be marked “Cyber Resilience Day 2025”: the day you boost the cyber secure backup capabilities at your company. It’s the next logical step from World Backup Day.



Cyber Resilience Year 2025

Cyber resilience, as important as ever in the world of data backup and recovery, should lie at the core of enterprise storage solutions with the capability to make cyber recovery of data virtually instantaneous. This can be game-changing for enterprises.

Highly available backup targets have become a necessity for enterprises. In addition to continually servicing backups, backup targets may need to facilitate fast restores and perform forensic analysis. This should ideally be based on a stateless recovery model to significantly reduce complexity. It makes it quick and easy to ensure your backup and recovery system is always highly available and fully optimized, while maintaining full data integrity.

If you’re thinking about cyber secure backup today, consider this question: What if it’s the way that your organization is backing up data that is the weak link? Ensure cyber secure backup is on your priority list.