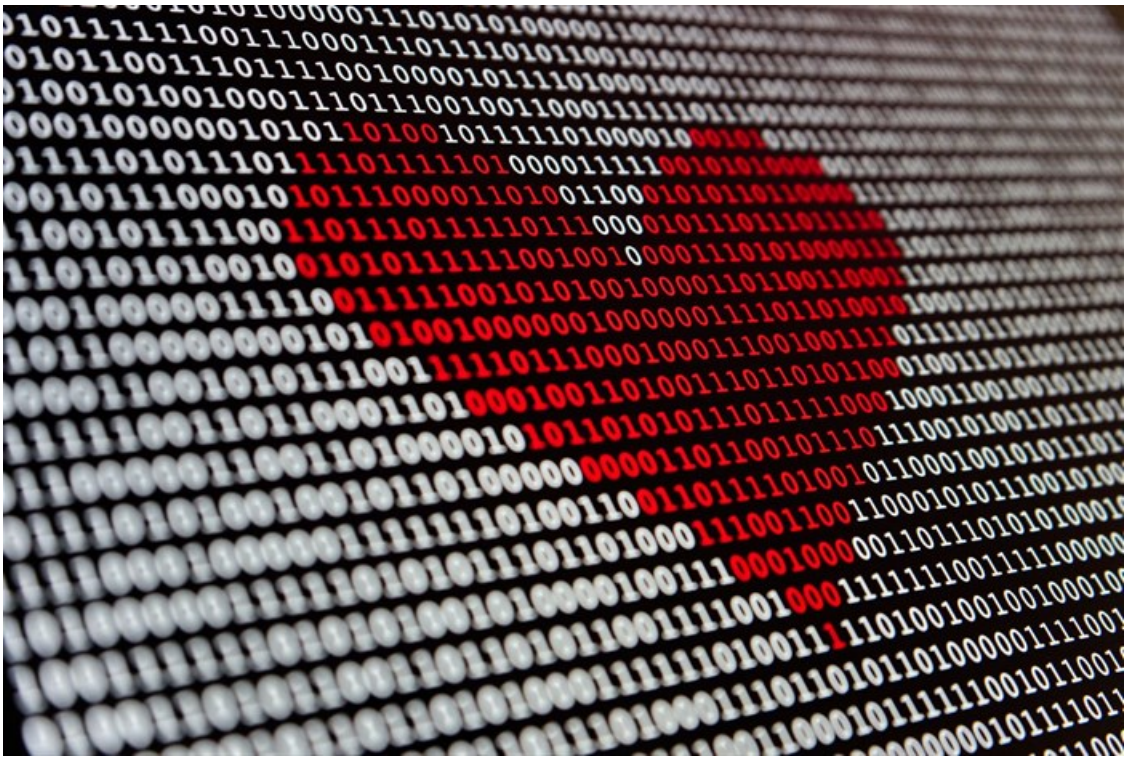
BIZCOMMUNITY

World Backup Day 2023: Key factors for modern enterprise backup

By Edwin Weijdema

29 Mar 2023

Since the inception of World Backup Day in 2011, technology and the data it processes have continued to advance. Enterprise organizations are more focused than ever on protecting and securing their data across complex IT environments. As we celebrate World Backup Day 2023, enterprises need to prioritise two key factors: cloud compatibility and reliable recovery.



Source: Unsplash

Cloud-compatibility

Firstly, a modern data protection strategy and the deployed backup solution supporting it must be able to protect workloads across any IT environment. The rise of cloud migration and affiliated services has meant that the physical data centre is no longer the heart of the IT infrastructure.

The *Veeam Data Protection Trends Report 2023* found that the average breakdown of servers is 28% in physical servers within a data centre, 25% on virtual machines (VMs) hosted within the data centre and 47% on VMs hosted within a hyper scaler or Managed Service Provider (MSP). This means that the modern environment is heavily dispersed, highly virtualised and mostly cloud-hosted.

Pointing out that most organisations have embraced hybrid cloud over the last few years may seem obvious, yet so many enterprises still rely on “legacy” backup solutions that were designed to protect physical on-site servers and are simply not fit for purpose in our hybrid world. These legacy backup mechanisms rarely yield good outcomes when protecting modern virtual or cloud-hosted workloads.

So why haven’t more enterprises pivoted to solutions that cover cloud-hosted workloads like Licensing as a Service (Laas) or software as a service (Saas)? It's partly because it's not the top priority for many - it typically has to start hurting before enterprises start moving.

An equally significant factor is that many of these legacy solutions have vendor “lock-in” making it harder for organisations to migrate their data to a different solution. When looking at backup solutions I would always advise looking at vendors without any kind of lock-in for this exact reason - you’ll never know when you need to change or move things around.

Reliable recovery

The other key consideration for enterprise backup is consistent reliability. Protecting business continuity and building resilience are the key reasons to invest in backup in the first place and if you’re looking at it as a compliance exercise, then you are looking at it the wrong way so naturally ensuring that the backup delivers is key.

There are two factors here; the reliability of the backup and the reliability of recovering data or workloads in the event of a disaster. Backup is your foundation, and as such, it needs to be 100% without any error.

If you're running a legacy backup solution not designed for a hybrid cloud strategy, reliability is naturally going to suffer. Other factors that determine the reliability of a backup, particularly when it comes to ransomware, are the number of copies being kept, having copies stored offsite, air-gapped (offline) and use of immutable backups (that are fundamentally unchangeable by ransomware or other malware).

Recovery is just as critical, however, and is often not spoken about as much. As a result, this is where we often see enterprises go wrong. You’d think backup and recovery go hand-in-hand (backup is what you use to recover after all) but there is often a disconnect which makes data recovery less reliable than needed.

This is due to how infrastructure is designed. Architecture built for backup might be able to duplicate 100% of its data and workloads in the space of 24 hours but when it comes to recovering this data and restoring it to the live environment, it might only be able to do 5% of this in the same time frame.

It's like a motorway with six lanes in one direction, but only a single lane going the other way. Enterprises need to start designing their infrastructure with recovery in mind to reduce downtime in the event of an outage or ransomware event and ensure they get the most out of their backups.

While many enterprises have made huge strides in how they think about backup, there are many who still have a long way to go. The backup needs to be transformed from an afterthought to the crux of the IT infrastructure. Building resilience to cyber-attacks or accidental outages is simply not possible without a modern backup strategy that is cloud-native and is built with recovery in mind.

ABOUT THE AUTHOR

Edwin Weijdema, field CTO EMEA and lead cybersecurity technologist, Veeam