How to be 'data ready' in 2020

By Johan Scheepers

4 Feb 2020

Data is an intrinsic part of business processes and also a source of competitive differentiation thanks to the potential of data analytics. Data has become a mission-critical business asset, which means that organisations need to be able to discover, protect and use it effectively and in a timely manner.

Johan Scheepers, Country Head at Commvault

This concept is known as being ‘data ready’. While there are many factors affecting an organisation’s data readiness, three key issues will be prevalent in 2020: ransomware, multi-cloud environments and data compliance regulations.

Tackling these key data issues can help organisations to be data ready in 2020.

Ransomware is rampant

Ransomware is a threat to each and every business today. In fact, it is so prevalent that an attack has become a matter of 'when' and no longer 'if'. High-profile data breaches were a common theme in 2019, and many attacks caused several days of service outages.

A new malware threat called 'wiper' is also becoming increasingly prevalent. This malicious software does exactly as the name suggests – rather than holding data to ransom by encrypting it, it actually erases it from its storage media. This changes the game completely.

A data wipe is not about money, it is completely malicious and an outright hostile attack. Paying the ransom or de-encrypting ransomed data by other means is not an option. If you do not have an effective backup and recovery solution in place, and you are 'hit' by a successful wiper attack, your data is gone.

The ability to recover from a malware attack involves more than Disaster Recovery (DR). Manual backups and attached storage can also be infected, which means that having multiple backups is no longer enough.

Being data ready in the case of malware means we have to think differently about business continuity. It is imperative to have strategies in place to detect anomalous behaviour within data storage as well as backups and archived, so that attacks can be identified quickly and suspicious behaviour can trigger alerts to notify the correct people.

The key to a data ready recovery system is rapid, frequent and separated backups that allow you to bring key systems back online immediately while you ascertain where an attack came from, isolate it and remove it.

Managing data in multiple clouds

Most organisations already exist in a multi-cloud environment, even if they are unaware of this fact. Whether it is a hosted Enterprise Resource Planning (ERP) solution, Office 365 or some form of cloud storage like Google Drive or iCloud, these solutions are frequently found in the makeup of businesses.

On the other side of the coin, there is also no organisation that is completely 100% in the cloud.

This multi-cloud hybrid scenario creates the need to be able to move data between systems. There are many reasons why data may need to be moved, either between clouds or between the cloud and the premises. The underlying common factor is that business models and needs change, so data architecture needs to be able to adapt. This is part of data readiness – the ability to drive economies between clouds and on premises solutions to maximise cost and benefit while minimising risk.

This in turn requires central visibility into all data across all of the various areas of storage. It is critical to data readiness to have a central management layer or platform in place to consolidate the view of data across the organisation. Without this visibility it is impossible to migrate data to leverage the best provider or location to meet changing business needs.

Meeting compliance requirements

Data is becoming increasingly regulated and it is not enough to know that you have the data, you also need to understand the purpose for which it was collected. Companies must have a record of the consent from the consumer to use the data for its intended purpose and the ability to comply with the 'right to forget' should the consumer request this. This is an imperative of all data privacy regulations.

Data readiness means having a way of consistently knowing where data is, what type of data it is and the sensitivity of the information. This requires specific tools, as manually identifying sensitive data is simply not possible given the volumes of

data in business today. It is also important to enable search and discovery to enable the ‘right to forget’ and then prove that the data has been removed, including from backups.

Be data ready in 2020

It is absolutely essential today to know what data you have, the purpose for which it was collected, and that it is adequately protected and can be recovered in the event of a data loss event. It is also critical to ensure that backups are protected and that they are tested to ensure that data recovery is possible.

Data readiness enables business agility by ensuring that data is available at all times in the right location to the right people. This means that your data can be leveraged to create business value. However, it is impossible to manage what you do not know exists.

Essentially, the ability to deal with pressing issues such as ransomware, the multi-cloud and compliance boils down to data governance and effective data management, which lie at the heart of data readiness.

ABOUT JOHAN SCHEEPERS

Johan Scheepers is Commvault systems engineering director for MESAT

- Why POPI compliance is not just an IT issue - 7 Dec 2020
- Data management is at the heart of cloud security - 1 Dec 2020
- Why is SaaS so valuable in a post-Covid-19 business environment? - 19 Nov 2020
- The perils of not knowing your data - 17 Mar 2020
- How to be 'data ready' in 2020 - 4 Feb 2020

View my profile and articles...