BIZCOMMUNITY

Data backup isn't dead, it's never been more important

By Jasmit Sagoo

29 Apr 2020

What businesses want from the cloud is changing. Pure cloud adopters fear vendor lock-in and we're increasingly seeing organisations spread the risk by utilising multiple cloud providers.

Jasmit Sagoo, senior director, head of technology UK&I at Veritas Technologies

In fact, our own research found that more than half (58%) of companies that currently use one cloud provider plan to expand their portfolio across multiple cloud platforms. This gives them the greatest chance to deliver the best, most responsive customer experiences.

Meanwhile, those running a hybrid model have the option of operating their most critical workloads on-premises and using cloud platforms for less sensitive transient data, data that feeds customer-facing applications.

To hedge their bets, some companies opt for a hybrid and multi-cloud approach, using their on-premises sites as well as a multitude of cloud environments, to ensure they have the best service outcomes whatever the circumstances.

A hybrid and multi-cloud framework may be the next stage in an organisation's evolution towards the cloud. Yet it poses an urgent risk if data protection and availability aren't taken seriously.

Trouble in paradise

As they continue their migration to the cloud, organisations have come to realise that different workloads are better suited to certain IT environments. When used strategically, these environments deliver a combination of greater speed, flexibility, agility, security and savings when organisations have visibility over their IT estate and pay close attention to matters like cloud usage.

A multi-cloud strategy has all the agility and scalability of the cloud without depending on a single provider. It gives businesses the ability to move workloads to other clouds in the event of a disaster. A hybrid approach, meanwhile, allows an organisation to reduce unexpected cloud costs and customise certain applications further than what's possible in the cloud.

It's a good option for companies that want to take full control over application and data availability, its protection and ability to have insights that provide visibility into operations and help ensure regulatory compliance.

However, if organisations aren't careful this greater flexibility comes at a price. Hybrid and multi-cloud environments are extremely complex: an application may have its tiers residing on multiple different clouds or physical data centres. This complexity only increases with the number of environments and applications businesses have. A highly complex and fragmented data environment is difficult to monitor and control, providing many points for failure and intrusion.

Businesses risk fragmenting their data management strategies and toolsets if they don't utilise solutions that can operate in hybrid environments, resulting in numerous overlapping and contradictory policies. Without a unified approach to data management and protection, businesses may find inconsistencies in not only the tools they use but also in their policies on retention of data, encryptions of data and most importantly recovery of their data in critical situations.

Many cloud service providers (CSPs) offer data protection services in a bid to become more competitive and capitalise on growing awareness around data protection. However, coverage differs drastically between providers when what organisations need is comprehensive protection across all environments.

In short, companies can't rely on their CSP to keep their data safe. The majority of contracts still place responsibility for data protection in the cloud on their customers. Yet this isn't clear to many – 69% of organisations still incorrectly believe data protection, privacy and compliance are the responsibility of the cloud provider.

It's worth remembering also that data protection regulations, like GDPR place responsibility for data loss on the organisation, not its cloud provider. Those that fall foul of the regulator face the prospect of considerable fines, reputational damage and the risk of shrinking market share. The only solution is for companies to take responsibility for their own data protection. A critical part of this is having a strong, well-defined data backup plan in place.

Preventing data downtime

A multi-cloud strategy can help spread the risk when it comes to downtime – if an application environment goes offline, it can be switched or failed over to run in another cloud or hybrid environment. The challenge always occurs should multiple complex applications go offline.

How would businesses recover their mission-critical services within the agreed SLA? Organisations need to plan on implementing both application and data availability but also application and data resiliency. The nirvana would be to have it

completely automated.

Organisations must also contend with ransomware. Once malware infects their system, it spreads like a virus. Ransomware can surge across a company's network, knocking out any onsite data centres one minute and blocking access to their private cloud the next. If a ransomware attack can't be contained, it rarely matters how many different environments you run.

A multi-cloud approach may be more flexible and efficient than relying on a single cloud, but its many moving parts can make security and governance highly complex. To resolve this, organisations need a backup plan.

The difference between backup and archiving

Chris de Bruyn 28 Apr 2020

Backing up the most crucial data and services ensures that any business interruption, whether it's caused by a server outage or ransomware attack, won't stop a business in its tracks or incur massive costs while they wait for systems to come back online.

The first step in delivering a strong backup plan is visibility. Organisations cannot protect what they cannot see. When data is visible it is easier to protect under a single, consistent set of policies, so investment in tools that link together disparate data environments and the infrastructure that supports it is vital for success.

The importance of protecting your data

Lukas van der Merwe 19 Mar 2020

The next consideration must be around simplification. Designing and implementing a data backup plan for every environment is time-consuming, counter-productive and inefficient. Every time a company's policies change, they'll have to be implemented individually for each environment at considerable cost. Businesses should seek a platform that can simplify and automate this process, rolling out consistent policies across their entire application and data estate.

Data is an organisation's greatest asset, and it needs to be managed and protected. In today's highly complex, hybrid and multi-cloud environments, the need for consistent and superior governance, protection and resilience across all environments at all times is essential. Adopting a platform that ensures businesses with visibility on their data, its location and whether it's being protected, helps maintain critical business services and, in return, their staff and customers.

A good data management plan delivers true peace of mind. It's about ensuring that companies have confidence and tools to ensure that, when something goes wrong, their data isn't lost in the machine. Far from rendering it redundant, the scale and complexity of tomorrow's hybrid and multi-cloud environments calls for a solid data protection plan which can only be made possible using a single tool that can span across all their environments.

ABOUT THE AUTHOR

Jasmit Sagoo, senior director, head of technology UK&I at Veritas Technologies