Hybrid Cloud Nirvana: Achieving the Balance to Drive Business Forward

How to avoid the pitfalls that derail the journey to the perfect hybrid cloud

A Commvault and Cisco eBook

COMMVAULT Be ready

CISCO

COMMVAULT Be ready

cisco

Contents

Introduction

Hybrid cloud is changing the world of business and in a rapid way. If cloud opened a new avenue for rapid IT service delivery, multi-cloud has created a new era in IT flexibility.

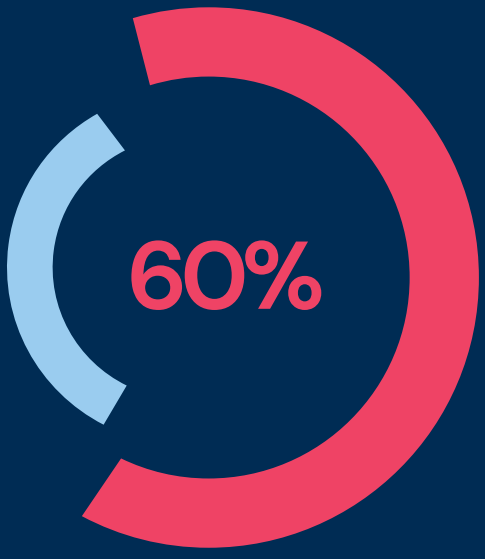
A multi-cloud architecture allows organisations to use the best infrastructure for the workload. Multi-cloud provides flexibility around where workloads can be hosted, such as on-premises, with a managed service provider or in a public cloud, in addition to how services are provisioned across IaaS, PaaS and SaaS.

For example, in a multi-cloud environment, web applications could benefit from the global reach of cloud, whilst Big Data processing can be performed with the power of on-premises equipment.

Whatever the workload, multi-cloud success will be underpinned by data availability and protection.

Globally, cloud-based data is growing at more than 60% per annum, compared with more than 30% for on-premises, according to IDC,[1] and failure to protect data across multiple locations and types of infrastructure will hinder an organisation's trust in the platforms and the potential for innovation.

This eBook, Data Management and Data Protection Built for Today's Hybrid Cloud World, is an essential guide, for IT and business leaders, to getting the most out of cloud, while keeping data safe.



[1] *https://www.networkworld.com/article/3325397/idc-expect-175-zettabytes-of-data-worldwide-by-2025.html*

An organisation's value is in its data and you need to protect it to be able to use it effectively. Without effective data management and data protection, downtime and data loss are a constant risk and teams cannot reach their productive potential.

A common misconception about cloud is customer data is well protected – it is important to read the fine print. Data protection can be worse in the cloud as often there is no native service from the provider. Moreover, some of the native offerings do not meet typical enterprise protection requirements.

A modern data protection architecture and platform does not simply mitigate risks, it removes barriers to innovation and time to new product development. However, the technology itself must be built for multi-cloud and be flexible enough to adapt to changing cloud services.

When managing data becomes second nature, people are free to add more value to their work today, and feel better prepared for tomorrow.

Digital transformation programs are driven by access to data and secure information interchange. Without flexible data protection an organisation's ability to modernise is stifled, along with its innovation potential.

The immediacy of cloud delivers business value, but left unmanaged cloud can expose risks of data loss and an inability to recover from a disaster.

It is time to take a holistic approach to data management by supporting on-premises, MSP and cloud delivery options, all while ensuring complete data integrity, automation, security and compliance.

IT disruption amid the shift to multi-cloud

IT is undergoing a fundamental shift. The move from legacy systems to hyperconverged and cloud-based infrastructure is happening quickly and cloud is being widely adopted for both infrastructure and applications.

With organisations looking for a cloud-like experience in the datacentre, including scale, agility and consumption-based economics, new technology is needed to deliver a consistent experience.

$4.6B ↑

Globally, private cloud spending reached $4.6 billion, a rise of 28.2 percent year-over-year, according to IDC.[2]

60%

Cloud-based data is growing at more than 60 per cent per annum compared with more than 30 per cent per annum for on-premises, according to IDC.

As cloud-based workloads have become core to an enterprise, the need to integrate with other applications has increased and every public cloud workload now is integrated with either the enterprise's own private cloud environment or that of a third-party provider.

There are big variations in data growth by industry and application. IoT workloads and the integration of operational technology applications with IT systems is a good example of high data growth. For example, IDC forecasts worldwide data will grow to 175 zettabytes by 2025, with much of it in the cloud.[3]

[2] *https://www.networkworld.com/article/3313319/private-cloud-spending-is-increasing-not-decreasing.html*

[3] *https://www.networkworld.com/article/3325397/idc-expect-175-zettabytes-of-data-worldwide-by-2025.html*

With all this growth, data is playing a critical role in business transformation. The value of data to business continues to grow and, accordingly, the value of business data to attackers is increasing.

With new threats constantly emerging, where data lives, what's creating it, and how it's stored, is becoming more complex to manage and secure across a multi-cloud.

Organisations are taking different journeys through digital transformation, and multi-cloud environments are arising as different buyers procure different services.

For example, with disaster recovery, IDC is seeing more organisations choose cloud instead of a second datacentre.

The shift to data-driven business is impacting national and global data protection legislation such as GDPR has heightened IT's approach to security and privacy.

Compliance is now a major activity and cost for most organisations, and external providers that offer a service with auditable compliance for industry or national legislation are proving attractive, IDC research shows.

New workloads can collect enormous volumes of data from sensors, all of which needs to be stored and analysed. The costs of on-premises and cloud storage must be justified for the type of application.

Despite no guarantee that on-premises data storage is safer than cloud, according to IDC, security is a major factor in users' choosing to invest in on-premises private clouds, because sometimes a public cloud provider's assurances about data protection are not enough to satisfy enterprise governance or legislative requirements.

The shift to multi-cloud is impacting traditional IT and data management and data protection by changing the business drivers to focus on outcomes rather than technology.

Business drivers including the cloud procurement model of renting rather than owning the infrastructure, which can reduce risk as large providers are generally more resilient and secure. This also brings more controlled and predictable cost models.

By choosing out-of-the-box solutions rather than building them from components, organisations can achieve faster time-to-market and leverage more research and development.

Businesses need agility and would rather procure IT faster than wait weeks or months for hardware delivery. This helps focus on the application and outcome rather than managing infrastructure and ancillary services.

Shifting to multi-cloud also reduces lock-in and enables more freedom of architecture choice. This is advantageous for distributed and decentralised offices where staff need to access data anywhere, anytime.

Problems with legacy and disparate systems include management complexity – from patching and security, to storage and capacity issues, inflexible hardware that is difficult to scale, and a higher risk of outages.

In the traditional model the business is hampered by lumpy, often unpredictable, capex purchases with more focus required on "business as usual" and uptime rather than innovation.

Organisations are adopting cloud to meet requirements for infrastructure, development (PaaS) and applications. Most public clouds, including Amazon Web Services and Microsoft Azure, allow organisations to mix cloud-native services with on-premises data to deliver modern, high-performance applications.

The future is cloud-agnostic, where the best tools integrate with all clouds, creating maximum customer flexibility and agility.

The business case for multi-cloud must include mitigating any challenges around security and responsibility (who owns what risk?), complexity, application performance and cloud lock-in. Data sovereignty and ever evolving data privacy laws must also be considered.

Holistic data protection wherever data lives

The path to cloud for most organisations involves a combination of new service adoption and migration of existing on-premises infrastructure. This multi-cloud mix is delivering new potential for business innovation, but also demanding a new approach to data management.

IT buyers are looking for platforms to simplify management, reduce risk and cost, and this should not be compromised in a multi-cloud environment.

As the move to multi-cloud and hybrid-cloud accelerates, it's vital that data protection strategies progress and that on-premises data management and protection take on cloud characteristics of agility, flexibility, and scalability.

According to IDC, the uptake of data protection for cloud-based services is increasing as no data is without value now and any breach (regardless of location) is potentially damaging.

Many early adopters of cloud rushed to move all their data there, only to realise it needed to be kept on-premises in a private cloud.

According to IDC, some companies are keeping up with data protection, but others are not. Those which must demonstrate compliance have no choice but to keep up, while others are playing catch up by adopting various measures to mitigate risks.

Customers must look to enabling cloud and multi-cloud data backups and protection in an agile, flexible and reliable way, in addition to protecting on-premises data from a single solution.

Separate backup and data protection solutions for on-premises and different clouds is not adequate as it weakens the organisation's ability to manage data and restore it in the event of a problem.

The realities of on-premises and cloud applications are the data must be protected, as a breach or loss incident can happen anywhere.

A common misunderstanding about cloud is that the data is always protected, or cloud providers have processes in place to retain customer data and recover it when required.

Most clouds operate a "shared responsibility model"[4] where the provider is responsible for the infrastructure, and the customer owns the data and risk associated with protecting it.

Even if the cloud provider took responsibility for data protection and offered SLAs around it, it is still good practice to protect your data in case of an event outside your control. This could be anything from a cyber-attack to a contractual dispute.

Customers are seeking simplicity in the cloud, yet must deal with increasing complexity to protect their data. There is a range of tools, including Azure Backup for Azure, Amazon Backup for AWS, Office 365 native protection, and those for Salesforce.com data. Most of them do not offer a solution comprehensive enough for the workloads or provide feature parity with those in the datacentre. The platform, or "simple", approach to the cloud often becomes a "spaghetti" architecture of backup products and scripts.

Many customers think cloud never experiences downtime – and, therefore, data protection is not required – and the provider protects their data, which is usually not the case.

Data protection can be worse in the cloud as often there is no native service from the provider. Moreover, some of the native offerings do not meet typical enterprise protection requirements. If a customer deployed the same production service on premises, they would never choose a data protection system with a similar offering to the native cloud services.

Some cloud backup services do not meet the enterprise requirements of leading analyst firm reviews because of limited market uptake and product capability. There is also the challenge of a lack of flexibility to restore data – some cloud backups do not allow protection of competing cloud workloads, or recovery to third-party cloud services.

Another popular misconception is snapshotting cloud data is enough for data protection. This is exactly the same cycle that was seen in the datacentre 10 years ago. Snapshots don't provide application consistency, are hard to manage and require scripting and customisation. Add to that an absence of monitoring, no guarantee of recovery (including meeting SLAs) and limited flexibility, and it is easy to understand why Commvault IntelliSnap™ technology has been a game changer.

[4] *https://aws.amazon.com/compliance/shared-responsibility-model/*

To fully realise the potential of hybrid, organisations need a modern approach to data protection, including during any migration of applications from on-premises infrastructure to cloud.

Storage for data protection is just as important as it is for production systems and, in the case of cloud, might be the only option for compliance and data loss prevention.

A lot can go wrong during a transition from on-premises to cloud or vice-versa. This includes inconsistent protection policies and capabilities. For example, enterprises might have a seven-year data retention requirement, but how do they handle old backups? There needs to be a process for recovery even if the original data source does not exist anymore.

Secondary storage and data protection systems are often very fragmented, which complicates management, increases risk and creates silos. This also increases cost and is often contrary to the primary drivers for projects and transformation programs.

Promote the need to align primary and secondary decision making. If there is a scale out architecture for primary storage, why not mandate that for secondary storage as well? Scale out primary architectures will quickly reach the limits of a scaleup secondary storage and data protection platform. This creates more silos, restricts growth and limits the value of the scale out architecture.

Avoid the risk of creating silos and not meeting capacity-performance requirements as the primary storage scales. Standardise on processes and application and infrastructure platforms that scale for data protection.

A scalable data platform is particularly important during the transition from on-premises to cloud. Data protection is important to avoid disruption to services during any migration to or from cloud.

Data protection portability

Given the strong uptake of cloud and desire for digital transformation programs, today's IT and business leaders need a data protection architecture that is flexible, scalable and easily managed.

There are now many options for data protection in a hybrid cloud world, but to avoid future hurdles, organisations should opt for a solution that is not tied to any type of infrastructure or data source and can be managed from a single interface.

A future-proof data protection architecture can support any application, any cloud and any scale to caters for organisations of every size.

Organisation have options for data protection, no matter where the data lives, from a single "pane of glass", including backups, DR and during data migration to cloud. Disaster recovery for different cloud platforms is important as it allows the organisation to be protected from a single cloud outage.

Look to get the most value out of integration solutions. For example, Cisco Hyperflex is a differentiator for Cisco when using Commvault. Both companies are accelerating the drive to truly hyperconverged, multi-cloud and hybrid cloud architecture.

Cisco and Commvault help organisations prepare for the future and help enterprise customers reduce IT and data management costs and complexity. In this case the value of the two solutions combined is a flexible, scalable, data protection architecture.

Keep options open for MSP delivery. You might not have the resources to run your data protection systems in-house and you don't need to. The Commvault scale out architecture delivers linear performance and customer growth for MSPs, which help customers protect their data in an on-demand way. Data protection that can be offered by MSPs.

With multi-cloud data protection, customers can expect a number of benefits and business outcomes, including consistent protection of data everywhere, one platform with no customisation to protect everything, and disaster recovery across platforms, regardless if it is on-premises or in the cloud.

Building a future-proof data protection architecture

A multi-cloud architecture promises a new era in IT flexibility and productivity, with new applications and services available to staff in any location and on any device.

For organisations to adopt hybrid cloud with confidence, risks must be reduced during transition and ongoing management. Security is paramount.

Starting with people, education of staff remains a key focus and understanding the necessity of following security procedures is essential to avoid many common breaches.

Tactical options such as encryption are available in virtually every cloud storage provider to encrypt data while it is in transfer, either through a browser interface or a storage providers' dedicated client to perform the encryption.

Many cloud services also offer key management solutions that allow you to control access. This may prove to be a better, or at least more reassuring, risk mitigation because you are in control over who has the keys.

Discover where the sensitive data resides, classify and define the data types, and create policies based on where the data is and which data types can go into the cloud and which cannot.

There are also automated tools to help discover and identify an organisation's sensitive data and where it resides.

Better automation and insights also drive productivity by increasing efficiencies and reducing error rates.

Demand better service level agreements from cloud operators and take advantage of modern storage technology to reduce the risk of downtime.

Building a secure set of configurations for specific workloads and linking them to change management processes via automated processes will minimise scope for human error or malicious attacks.

Data protection options should all be spelled out in the SLA and include a description of the services to be provided and their expected levels of reliability. The obligations and responsibilities of each party – and remedies or penalties for failure to meet those metrics – should also be covered.

Insights about application recoverability and comprehensive support for applications and multi-cloud environments are important for optimising data protection.

A data platform to provide insights into data through indexing and eDiscovery also reduces risk by ensuring compliance to various business and regulatory requirements such as GDPR laws.

Conclusion

Data protection is highly critical in the move to cloud and could mean the difference between a highly optimised, manageable architecture and a sprawl of data and services which exposes security vulnerabilities. And once you have migrated to cloud, there are ongoing data protection requirements.

Organisations need to protect any application, on any cloud, at any scale. When Cisco infrastructure is combined with Commvault® software, it becomes the solution you need to make sure your data is available, moveable, and recoverable — when and where you need it. It also ensures your data lives on the most cost-effective and scalable infrastructure, including for mission-critical and enterprise applications.

Commvault can accelerate migrations and reduce risk with a broad coverage of data protection options, including popular storage systems, operating systems (including endpoints), applications and databases, virtual infrastructure, large files and Big Data, and SaaS and cloud-native data.

ScaleProtect™ with Cisco UCS® gives you a future-proof alternative that sets you free from ever-growing stacks of purpose-built appliances. By consolidating and eliminating your data silos, you'll shrink your on-premises hardware footprint, gain massive agility and finally have that holistic, big-picture view of your data you've always wanted, wherever it's stored.

Keep options open for MSP delivery. MSPs can be part of a multi-cloud mix and help protect data in an on-demand way.

The Cisco Commvault multi-cloud solution delivers the ability to accelerate adoption of multi-cloud by reducing data sprawl with policy-based automation of copy data management.

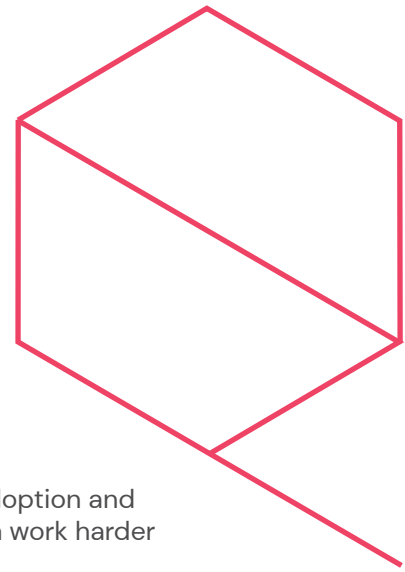
Remove operational complexity and gain more value from your data with native automation and orchestration capabilities — from on-premises to the cloud.

With ScaleProtect with Cisco UCS, you also benefit from: Greater resiliency and availability for more predictable performance and improved service level agreements (SLAs); Faster time to production with easy acquisition and rapid, on-demand deployment ending costly and complex forklift upgrades.

Commvault delivers faster capture of data and less disruption to production systems with snap-assisted backup. This solves the VMware “stun problem” (reduces potential backup failures), eliminates time consuming scripts, leverages VMware best practices (ensures security protocols are followed), and helps meet demanding SLAs.

Discover where the sensitive data resides, classify and define the data types, and create policies based on where the data is and which data types can go into the cloud and which cannot. Automation can help here.

Look for at least 50 per cent reductions in data protection footprint, manual effort and costs compared with traditional solutions.



The benefits of a modern approach are clear. There is a drive to increased adoption and innovation, improved productivity and reduced risk. And by making your data work harder you will gain invaluable insights for your business.

Cisco and Commvault help organisations prepare for the future and help enterprise customers reduce IT and data management costs and complexity. The value of the two solutions combined is a flexible, scalable data protection architecture.

About the Cisco / Commvault partnership

About Commvault

Commvault is a leading provider of cloud backup and recovery, and data and information management solutions. We help organisations worldwide to protect their data, and also derive greater business value and insight from it. With the Commvault Data Platform, customers modernise their IT operations, significantly increase efficiency, and better leverage their data. Our solutions and services are delivered directly and through a worldwide network of partners and service providers. Commvault solutions comprise one of the industry's leading portfolios in application and data protection, disaster recovery, cloud, virtualisation, governance, search/analytics and endpoints.

For more info, please visit: www.commvault.com.

About Cisco

Cisco brings together networking, security, analytics, and management. We deliver cloud solutions that span your multi-cloud world, from your on-premises environment to your multiple cloud providers, and from your applications to your infrastructure.

Our cloud solutions help you manage a private, hybrid, or public cloud, or all of the above. Whether you have one application and one cloud or multi-cloud applications and multiple clouds, we help you embrace a multi-cloud world by simplifying how you connect, protect, and consume your clouds.

- Consistent network policy across multi-cloud: Exclusive integrations with public cloud platforms that enable consistent network and security policy across IT-managed data centers and public cloud.
- Foundation for multi-cloud infrastructure: Hybrid computing stacks co-developed with leading public cloud providers that bring cloud services on-premises to power cloud-native applications and rapid innovation.

For more information, please visit: www.cisco.com.