Achieving Data Freedom in a Multicloud Environment

rackspace technology®

NetApp®

Achieving Data Freedom **in a Multicloud Environment**

While computing and data storage has been shifting to the cloud for 15 years, the COVID-19 pandemic fueled an increased reliance on virtual applications and cloud-based environments.

The Flexera™ 2022 State of the Cloud Report illustrates the growth in cloud dependence, with two out of three respondents (66%) indicating a higher-than-anticipated reliance on the cloud for business operations and data storage, and one in five (21%) rating this reliance as significantly higher than in previous years. Analysis by both Flexera and Statista reveals that almost 90% of enterprises have adopted a multicloud environment to manage their current workload and storage needs.

With businesses now relying heavily on applications and data storage in the cloud, the operational roadmap must shift to cost-effective solutions that provide secure, access to run workloads across multiple cloud environments. It is no longer a question of whether the cloud environment should be utilized for business functions. The focus now is on accessibility without penalization, or data freedom.

Defining Data Freedom

Data freedom at its most basic level is access to data with minimal restrictions or penalties. However, the surge in remote work, coupled with expansion of businesses in scope, scale and geography and the resulting prevalence of multicloud environments drives additional considerations: portability, integrity, agility, security, and cost.

As users tend to move from application to application, often many times throughout the day. That means business data must be agile and secure so that employees can log into a remote work environment or company VPN and access their files quickly and securely. Employees must be able to rapidly acquire, scale or evaluate data across multiple platforms. As cloud-based tools and applications become more prevalent — and a workforce relies on more than one cloud environment to meet objectives — legacy systems will not be sufficiently robust. The ability to access and analyze this data has become both more complex and more essential.

That access must be more than just a matter of convenience. Businesses must be able to access their data and applications with minimal restrictions and costs. That necessitates a solution that minimizes or eliminates egress fees that inhibit the ability to move data from one cloud environment to another. This means the computation of data must be regionalized and distributed to the cities closest in proximity to the user.

With proximity to data, businesses also need an improved user experience. It is no longer enough to simply provide end users with access to the cloud. The process must remain simple enough that users of all levels of computer literacy have easy access and can work efficiently with data.

Compliance also must be factored into cloud-based solutions, with consideration for the latest protocols and privacy directives, including government mandates like HIPAA and the General Data Protection Regulation. As the federal government implements those directives, businesses will need to adopt them and comply if they want to contract or partner not only with federal agencies but with other businesses that do so.

Finally, as breaches of online data proliferate, security measures must remain a top priority. As businesses take steps to make data more widely and easily accessible, they must address the resulting vulnerabilities as it transfers from multiple clouds to key applications. Security protocols need to control both access to the data and users' movement in the multicloud environment.

Considerations for Achieving Data Freedom

For a company that has adopted a multicloud environment, or is assessing whether to do so, the first step toward achieving data freedom is determining its best data fit — the cloud, a data center, or the edge? Nearly four out of five decision-makers incorporate multiple public clouds, with most integrating a hybrid approach that encompasses both public and private access. Increasingly, companies are finding the cloud offers the advantages of rapid scalability, reduced capital expense, ease of access, and the ability to stay ahead of both software and hardware update cycles.

The need for data mobility is another key driver for data freedom. If a company's data resides in multiple cloud environments and across multiple devices, it must remain mobile within a neutral environment. Utilizing a central cloud repository in a cloud-neutral zone achieves that goal. It also saves money in potential egress fees and can prevent penalization for inadvertent non-compliance with local or federal requirements.

Creating a data fabric is an additional step toward ensuring consistent enterprise access across hybrid and multicloud environments. This architecture standardizes data management practices across public and private clouds, on-premises and in edge or IoT devices. Its integration helps to ensure the security, visibility, protection, access and control of business data and applications, regardless of where they reside.

The effectiveness of the organization's IT infrastructure is another factor. Latency issues can arise both in the storage of data and in accessing and transferring it, so businesses need to examine both storage bottlenecks and cloud connections. Companies also need to examine optimization of data centers. A regional edge data center provides closer proximity to users, reducing latency and increasing efficiency.

Benefits of the Rackspace/ NetApp Partnership

The management of cloud-based architectures is complex, and given the continued growth in cloud adoption, the need to manage cloud resources while ensuring compliance, security and maximum cost savings is critical. The partnership between Rackspace Technology and NetApp helps businesses achieve data freedom while limiting the ever-increasing cost of fees for data stored or transmitted within a public cloud environment.

The Rackspace Data Freedom platform disaggregates storage from the public cloud, helping businesses retain data ownership and avoid unpredictable egress fees. NetApp's data storage solutions ensure the central storage of business data outside a specific cloud provider, making it available for fast and private transport through any cloud service. The use of multiple private, low-latency connections via Rackspace Technology's RackConnect GlobalTM network not only aids in cost management, but also ensures a seamless experience for the end user.

Next Steps

Although the pandemic escalated the use of cloud solutions for software applications and data storage, this concept is certainly nothing new. Global decision-makers currently manage almost half their workloads in the cloud and expect to increase their reliance on cloud-based platforms over the next year. The use of the cloud is a key factor in cost savings, as is the transition from on-premises software to SaaS alternatives. With the right architecture in place, businesses can achieve the desired goal of data freedom.

Rackspace Technology provides multicloud solutions, and NetApp provides a state of the art storage offering to ensure the delivery of the right data to your business and its employees at the right time and place. Interested in learning more about the Rackspace Technology and NetApp partnership and its secure, seamless approach? Contact Rackspace Technology today.

Resources

- Flexera™ 2022 State of the Cloud Report
- Multi cloud adoption worldwide in 2021 and 2023, by organization size (Statista)
- What Is a Data Fabric? (NetApp)
- Why Rackspace Technology?
- Rackspace Technology Data Freedom
- Data Freedom (Rackspace)