White Paper

Multi-cloud Data Protection-as-a-service

The HYCU Protégé Platform

By Christophe Bertrand, ESG Senior Analyst

November 2019

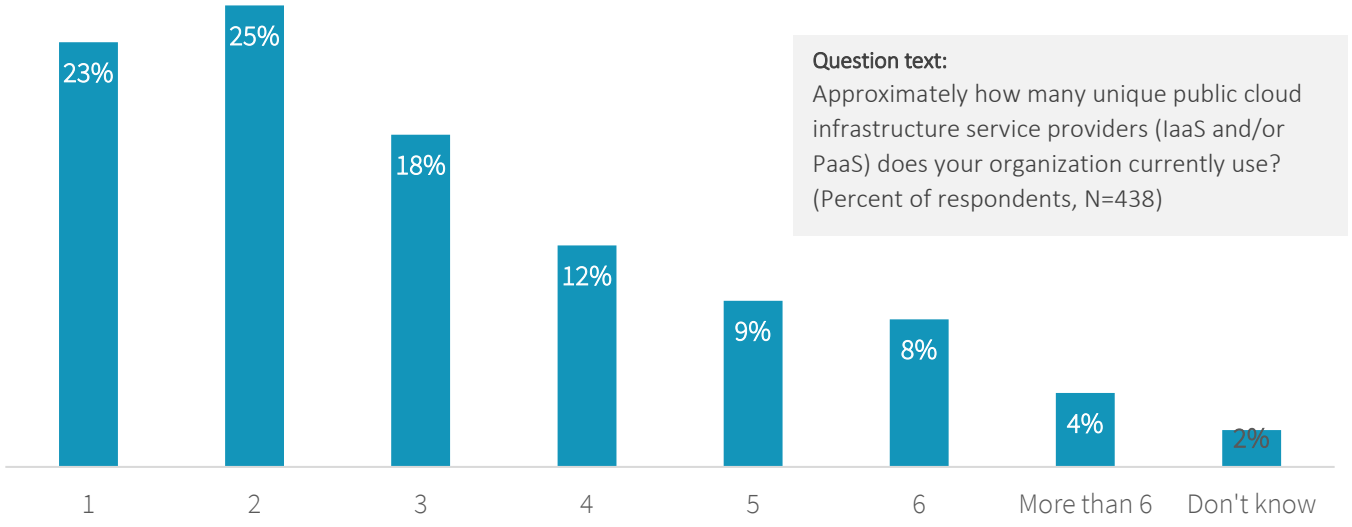
This ESG White Paper was commissioned by HYCU and is distributed under license from ESG.

Contents

A Multi-cloud World

It would not be an overstatement to say that our global economy literally runs on cloud infrastructure at this point in time. Use of the cloud is generating numerous opportunities for organizations to improve their business capabilities, modernize their processes, optimize their efficiencies, and become more data-centric. However, the advent of cloud is one of the reasons that 66% of ESG research respondents indicated that IT is more complex today than it was two years ago. Modern enterprises typically leverage multiple cloud infrastructures. According to ESG research, more than three-quarters of current public cloud infrastructure users leverage more than one cloud service provider in 2019 (see Figure 1).[1] Multi-cloud infrastructure is the new norm.

Figure 1. Multi-cloud Is the New Norm



Source: Enterprise Strategy Group

There are many reasons to use multiple public cloud providers:[2] Thirty-five percent of organizations report wanting to select the best fit for each application or workload as one of their reasons for using multiple cloud providers, closely followed by 33% who said they want to leverage cloud services and applications provided by their large software vendors. Not far behind are the 32% who said that they use multiple cloud providers for risk mitigation and higher availability, and another 32% who are simply "hedging" their bet: not wanting to be dependent on only one cloud provider.[3] Let's explore some of the challenges that IT organizations face today in this multi-cloud context.

Current Approaches Present Challenges

Extending on-premises environments to cloud infrastructures is a common strategy that originated in a quest for efficiency and simplicity. As is often the case, technology, business processes, and people skills do not always evolve at the same pace, resulting in additional complexity for IT. Many applications are now born in the cloud "first," while others are migrated from traditional on-premises environments. ESG research highlights that some of the most pervasive challenges

[1] Source: ESG Master Survey Results, *2019 Technology Spending Intentions Survey*, March 2019.
[2] Source: ESG Brief, *The Current State of Multi-cloud Strategies*, April 2018.
[3] Source: ESG Master Survey Results, *The Emergence of Multi-cloud Strategies*, April 2018.

organizations face when it comes to the usage of public cloud revolve around risk and compliance management and cooperation between the cloud operations and IT domains within the organization.[4]

Add multiple clouds to the mix and now the question becomes one of optimized provisioning and performance fit. Geographic considerations also come into play from a data residency perspective as well as for compliance risk mitigation.

At the heart of this new layer of complexity and challenges is the fundamental question of application and data protection. How do you protect and recover assets such as business-critical applications and virtual machines in multi-cloud environments? In addition, SaaS applications offer their own set of challenges. Traditional methods for backing up applications just do not apply, but protecting data still remains the responsibility of the data owners and not the service providers.

Not every cloud infrastructure is born equal, or to put it a different way, how you protect business-critical applications is likely to vary widely across clouds. Just like in the traditional on-premises world, choosing the best solution for protecting a specific workload or application makes a difference in multi-cloud environments, as well. It should also be mentioned that many organizations are not going 100% to cloud. Indeed, it is ESG's opinion that most organizations will end up in a hybrid IT configuration, combining on-premises infrastructure with multiple clouds as they adapt and adjust the IT infrastructure to the business's requirements and its digital transformation needs.

Modern organizations that leverage multi-cloud environments must be able to deliver similar recovery time objectives and recovery point objectives for their critical applications that run in the cloud. Think of it as disaster recovery coherence across clouds. In order to do so, they need to provide the best level of protection for each specific environment, rather than a "catch-all" solution that will likely not deliver against those service levels.

Complexity typically stems from having to manage multiple silos. As organizations embark on selecting the right approach for protecting multi-cloud environments, they need to consider solutions that provide a broad spectrum of coverage in order to minimize operational inefficiencies and associated costs. In addition, they need to provide consistent disaster recovery as one of the items in the equation.

There are a number of limitations today keeping organizations from not only lifting and shifting from one cloud to another but also migrating across clouds. Organizations need the flexibility to leverage multiple clouds and move applications and workloads around freely, whether for data reuse or for disaster recovery. This is where the HYCU Protégé platform comes in.

The HYCU Protégé Platform

The HYCU Protégé platform was designed from the outset to tackle multi-cloud data protection and data management challenges. It is focused on three original use cases that address the most salient pain points today: cross-cloud disaster recovery, cross-cloud data migration, and cross-cloud application recovery. We expect to see more use cases in the future.

The solution is positioned as a complete multi-cloud data protection and disaster recovery-as-a-service solution. It includes a number of capabilities that make it relevant and notable compared with other approaches in the market:

- It was designed for multi-cloud environments, with a "built-for-purpose" approach to each workload and environment, leveraging APIs and platform expertise.
- It is designed as a one-to-many cross-cloud disaster recovery topology rather than a one-to-one cloud or similarly limited topology.

[4] Source: ESG Master Survey Results, *The Emergence of Multi-cloud Strategies*, April 2018.

- Protégé is designed for the IT generalist. It's easy to use, it includes dynamic provisioning on-premises and in the cloud, and it can be deployed without impacting production systems. In other words, no need to manually install hypervisors or agents.

- It is application-aware and will automatically discover and configure applications. Additionally, it supports distributed applications with shared storage.

The centralized management capabilities afforded by Protégé and its capabilities for DR will help organizations improve operational efficiencies and operational recovery in a more coherent and consistent fashion.

The Bigger Truth

Multi-cloud environments are here to stay and will keep on growing in diversity, use cases, and, of course, size. Data growth is not stopping anytime soon, only making the problem more acute.

HYCU has taken a very different approach from many traditional vendors by selectively delivering deeply integrated solutions to the platforms they protect, and is now moving to the next challenge of unification and simplification with Protégé, calling it a data protection-as-a-service platform.

It credibly solves many challenges in current topologies associated with centralized management, or lack thereof, for multi-cloud environments. More importantly, the platform opens up the ability to go beyond recovery to deliver data reuse and intelligent data management options in the future. Use cases such as test/dev, compliance, and analytics come to mind.

HYCU's ability to execute and deliver on its roadmap has been very impressive. While the solution is new in the market, we expect to see a growing number of adopters in the next few months.