Simplifying Multi-Cloud Data Protection, Data Migration, and Disaster Recovery

Ed Tittel

CONTENTS

IN THIS PAPER

HYCU helps organizations safeguard their data, applications, and operations using consistent, coherent multi-cloud management and migration capabilities. It combines purpose-built components for each cloud platform that delivers a unified user experience for users and administrators alike.

This tech brief explores how HYCU Protégé enables companies to achieve business continuity, data protection, and resilience across cloud platforms from:

- Amazon (AWS)
- Microsoft (Azure)
- Google (GCP)
- VMware (VMware Cloud)
- Nutanix

At the same time, HYCU Protégé helps organizations manage cost without requiring duplicate or extra software licenses, redundancy, and hardware costs.

Modern organizations face a bewildering array of platforms and technologies through which they conduct their business. Above all, they must maintain operations and keep applications and data available, whether on-premises, in a private or public cloud, at the network edge, or in the network core. This means organizations must continuously back up their data, state, applications, and infrastructure, and be ready to recover those things to an appropriate location at a moment's notice.

This tech brief breaks down the support organizations need for protecting their operations into the following requirements:

- **Data protection:** Ensuring the integrity, validity, and availability of data to authorized parties, along with the tools to manage its access, integrity, and availability.
- **Data migration:** Moving data from one location to another, one format to another, and one application to another, where such locations may be on-premises or in one or more clouds, private or public. The latest Flexera State of the Cloud 2021 report found that more apps are siloed on different clouds (49%) than are integrated between clouds (45%), but that workload mobility between clouds (42%) is increasingly common.
- **Disaster recovery:** Capturing data, applications, and state information so that interruption of access or service in one location can fail over to another location, subject to pre-determined durations for interruption (recovery time objectives, or RTOs) and the tolerance for data loss (recovery point objectives, or RPOs). Flexera reports that nearly half (45%) of enterprises are already using some form of cloud-based Disaster Recovery as a Service (DRaaS).

These three requirements in many organizations are *multi-cloud*: a combination of two or more clouds that may be public or private, with the necessary software to ensure that workloads and their data can operate in any and all of those clouds. According to the Flexera report, 76% of enterprises use multiple clouds (one or more public and one or more private). A *hybrid* cloud solution combines on-premises and multi-cloud use cases into a single, integrated use case. Modern data solutions bring data protection, data migration, and disaster recovery—all cloud-based—together in an "as-a-Service" format.

One of the biggest business drivers for organizations to modernize their IT infrastructures is a need to escape the confines of legacy systems. Commonly, legacy systems don't support access to a cloud environment, or offer only limited cloud integration, whereas the organization needs to easily migrate workloads across multiple environments. Legacy systems might also offer few or highly limited capabilities for data protection or disaster recovery.

> **Organizations must continuously back up their data, state, applications, and infrastructure, and be ready to recover those things to an appropriate location at a moment's notice.**

Here's an "acid test" against which to measure your current IT infrastructure and its capabilities to support multi-cloud deployments, data protection, and disaster recovery. If it takes more than a sentence to explain how any of those elements work in your environment, your organization likely needs a more modern, capable, and simple solution. Such a solution must incorporate purpose-built, application-aware backup and data protection. Indeed, data recovery with infrastructure coverage is key to supporting modern infrastructure, modern workloads, modern apps, and modern data protection. Let's examine these cornerstones more closely, to make their relevance crystal clear.

Data Protection

It's hard to overstate the importance of safeguarding an organization's data, its most valuable asset. As an example, consider the potential impact of data loss, unwanted breach or disclosure, or denial of access

through ransomware attacks. According to a 2021 IBM/Ponemon Institute study as reported in a recent SecurityIntelligence blog, the average cost of a data breach in 2021 is $4.24 million, and the cost for a ransomware attack comes in at $4.62 million, so these losses are more than hypothetical.

> **An organization must do what it can to ensure that data remains protected throughout its travels and uses, on-premises and in all clouds, private and public.**

Next, consider the importance of the business systems that access your data, which may be tightly interwoven into one or more cloud environments. That same importance conveys equally to mission-critical applications, databases, and virtual machines (VMs). It's vital to safeguard all these elements from unauthorized access, attack, loss, or other harm to ensure ongoing business operations. Making life both interesting and more than slightly scary, the threat landscape changes daily. So organizations require solutions that can handle advanced, zero-day attacks and that keep up with current threat intelligence and prioritized attack vectors.

In short, an organization must do what it can to ensure that data remains protected throughout its travels and uses, on-premises and in all clouds, private and public.

Data Migration

Data migration actually spans an entire spectrum of possible use cases. These can be as simple as "lift and shift" migrations of applications from on-premises into one or more clouds, or from one cloud environment to others. Migrations can get complex if they involve multi-dimensional workloads, often calling for open, extensible frameworks or container platforms that stay consistent wherever they run, on-premises or in the cloud.

Once organizations bite this bullet and accept the time, cost, and effort involved in a modern data migration, they can exploit numerous benefits that come from rationalizing the migration of workloads and their data. These include:

- Scaling up and scaling out (sometimes called "cloud-bursting") to accommodate occasional, periodic, or cyclical peak demands.
- Exploiting public cloud storage for off-site backup, to provide a variety of potential recovery scenarios with the goal of painless business recovery (see the next section for additional discussion of this important topic). Recovery might be to the same public cloud, and possibly to others.
- Recovering specific applications into another cloud for testing and development, as well as for disaster recovery or cloudbursting as circumstances dictate.

> **Managing data across multiple clouds coherently and consistently helps organizations achieve additional synergies and advantages.**

At the same time, managing data across multiple clouds coherently and consistently also helps organizations achieve additional synergies and advantages, including:

- Supplying data for multi-cloud use cases (e.g., to support data sovereignty or residence requirements in specific countries).
- Employing data protection applications that can support both move and copy operations for quicker, easier scale-up and scale-out, to support enhanced resilience and availability, or to provide end users with best-case latency and performance.

To make such data management consistent and coherent, both management and migration must deliver an acceptable user experience in each cloud, and a unified and workable user experience across all clouds. The best

solutions expose a common overlay atop purpose-built solutions for each cloud. This makes the user experience and interface identical to how administrators and users handle other tasks, particularly those involving communication between clouds and management across clouds. Behind the scenes, purpose-built tools facilitate copy and move operations for workloads and their data across multiple cloud domains.

Disaster Recovery

The implementation of disaster recovery involves careful consideration, good design, and careful testing to validate that business keeps going even when the IT infrastructure fails or becomes inaccessible. Primary drivers for workable disaster recovery include common threats discussed earlier, especially those that come from social engineering, phishing, and ransomware attacks. Modern disaster recovery also leans heavily on purpose-built solutions that support and protect whichever clouds, public and private, the organization is using. Disaster recovery solutions must be affordable while ensuring business continuity for all of the apps, data, and services in use at an organization.

For a proper, modern solution to do its job, organizations must make sure that the cloud platforms in which they invest operate as they're supposed to, buttressed by integrated backup and recovery tools and techniques. To keep cost and complexity down, such solutions should involve no deliberate redundancies, extra software licenses, or hardware costs. In fact, the best data protection solutions should enrich whichever clouds the clients choose, rather than requiring separate runtime environments in which to operate. A proper solution uses simple technology to recover production VM disk image files, captured using period snapshot mechanisms. Thus, such a solution works across all scales of operation, from small and midsize business to enterprise, government, or service provider (ISP, MSP, telco, and so forth).

Let's take a "lift and shift" backup and disaster recovery scenario for Google Cloud Platform (GCP) as a case in point. Whether an organization uses private, public, or hybrid clouds, Software as a Service (SaaS), or Infrastructure as a Service (IaaS), one of its prime objectives is safeguarding its data. GCP users understand that a flexible solution that meets changing needs and use cases is key. Disaster recovery works best if it's simple and cloud-native and delivers agentless application awareness to its users. HYCU Protégé addresses such needs in its approach to multi-cloud data protection. It provides a simple "lift and shift" mechanism to re-site applications (and their data) from on-premises or in-cloud operation to a different cloud. What's more, it makes sure data remains protected during and after migration, safely and securely. HYCU Protégé also enables organizations to recover specific applications onto a different cloud (or cloud region) for testing and development. This provides cost-effective disaster recovery across multiple clouds.

The process occurs in four steps, as follows:

- Recover production VM disk image files.
- Download and install the Google Cloud SDK.
- Create buckets and upload VM files.
- Import VM disks to custom images.

Please read the case study for additional details and technical instructions for each step. The process is simple, quick, and intuitive, and shows how HYCU supports GCP directly and easily.

> **For a proper, modern solution to do its job, organizations must make sure that the cloud platforms in which they invest operate as they're supposed to, buttressed by integrated backup and recovery tools and techniques.**

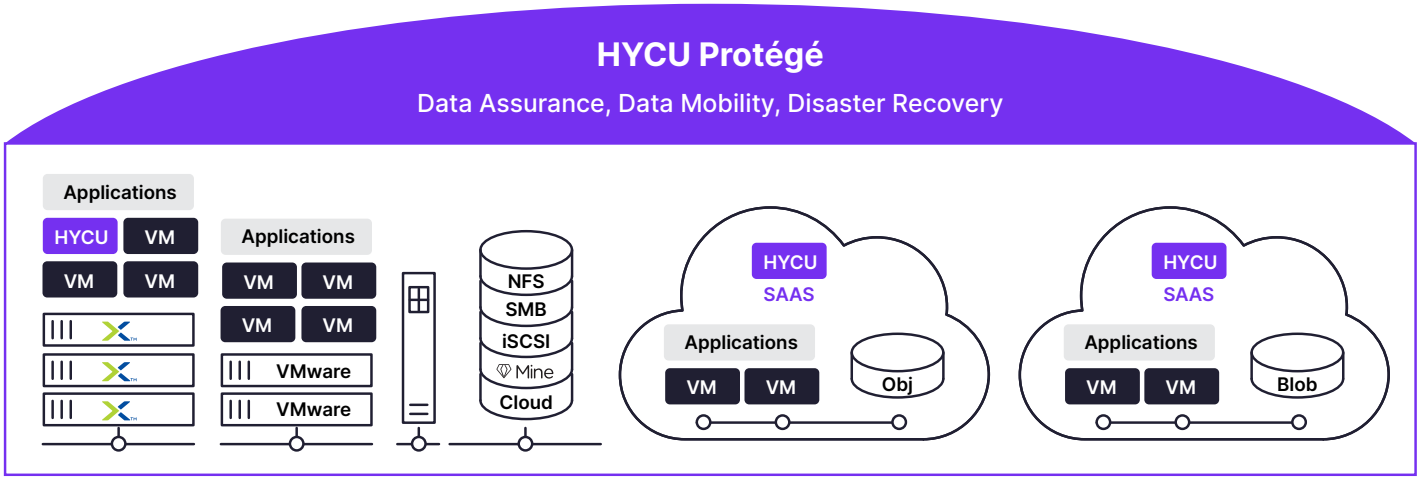

Figure 1: HYCU Protégé makes DR easy across a broad range of public clouds and computing platforms

Benefits of Simplicity and Consistency

HYCU provides simplified, application-consistent business continuity for an organization's data protection environment across multi-cloud infrastructures, from on-premises to public cloud.

> HYCU provides simplified, application-consistent business continuity for an organization's data protection environment across multi-cloud infrastructures, from on-premises to public cloud.

Companies can protect data in on-premises and public cloud environments such as GCP, Microsoft Azure, and Nutanix-based data centers. In addition to storing data, VMs, and apps to cloud targets, HYKU's solutions help ensure data resilience by seamlessly migrating VMs between on-premises and cloud infrastructures. Should disaster strike, HYCU provides recovery for mission-critical data to the cloud service suite of choice.

Figure 1 shows how HYCU brings multiple cloud environments together.

Says Simon Taylor, HYCU CEO, HYCU Protégé "allows customers the freedom to use the cloud their way, with their control. All from a single management framework that provides the best of the on-premises and public cloud environments they experience." In the same vein, Mr. Taylor emphasizes that clients run this show: "Your data. Your Cloud. Yours to control."

Sign up at HYCU.com for a free trial, or request a demo of our market-leading, SaaS-oriented multi-cloud data protection and backup and recovery solutions.