

Solution Showcase

Data Protection Strategies for Google Cloud Platform with HYCU

Date: September 2019 **Author:** Christophe Bertrand, Senior Analyst

Abstract: Cloud infrastructure and services adoption is accelerating at most organizations. Many key business workloads are moving to the cloud and need to be backed up. There is, however, a gap of confidence when it comes to backing up cloud data. IT needs new instrumentation for platforms like Google Cloud Platform (GCP) to protect data assets. HYCU offers an innovative solution for protecting GCP environments: It is natively developed on and for the platform, delivers enterprise-class features like the ones expected on-premises, and comes as a service.

Cloud Is Here to Stay

Cloud infrastructure and services adoption is accelerating at most organizations: 58% of organizations now report using public cloud in the form of infrastructure-as-a-service—in 2017, this number was 42%. And ESG research shows that surveyed organizations most often cited public cloud infrastructure services as an area of *increasing* IT spending, as they keep digitally transforming. Cloud is clearly here to stay. In fact, cloud-first strategies are becoming more prevalent, with 39% of organizations favoring this approach for deploying new applications (versus on-premises), a meaningful 10% year-over-year growth.

Many mission-critical workloads are moving to the cloud—and not just office productivity type of applications. Core business applications are now deployed in the cloud (see Figure 1). Other application services also now take place in public cloud infrastructures like Google Cloud, such as Cloud SQL, SAP Hana, and Big Query, with running production applications and business intelligence queries coming in as the most cited cloud use cases for 2019. In addition, 76% of organizations report using multiple cloud service providers.¹

With applications moving to the cloud, their associated data sets must also meet internal and compliance requirements and be subject to IT best practices.

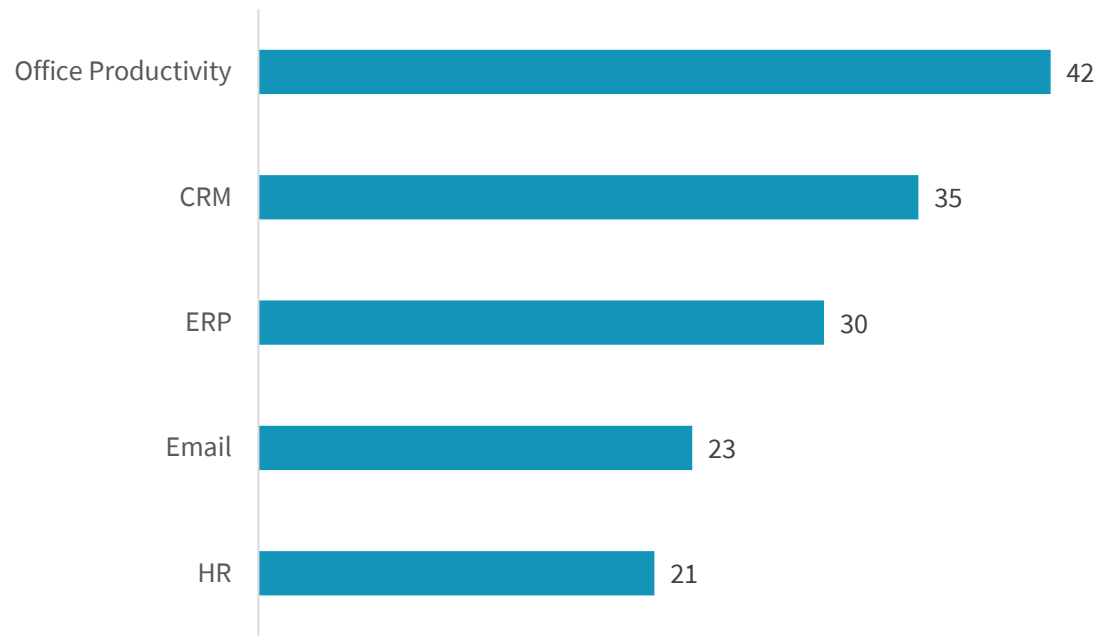
¹ Source: ESG Master Survey Results, [2019 Technology Spending Intentions Survey](#), March 2019.

This ESG Solution Showcase was commissioned by HYCU and is distributed under license from ESG.

© 2019 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Figure 1. Top Five Workloads Most Likely to Move to Cloud/SaaS in 2019

What applications currently running on-premises are your organization's highest priority to move to public cloud services? (Number of mentions, up to three responses allowed, unaided recall, N=600)



Source: Enterprise Strategy Group

Unfortunately, considering the many applications in the cloud and growing volume of associated data, misconceptions about protecting data in the cloud propagate, which ESG believes may be rooted in a conflation of service provider service level guarantees with actual (and more importantly, best practice) backup and recovery.² In other words, do not confuse cloud availability service levels with backup of your data in the cloud. Cloud data protection is not changing the age-old requirement of backup and recovery, despite the new set of challenges that protecting data in the cloud presents.

Cloud Data Protection: A New Set of Challenges

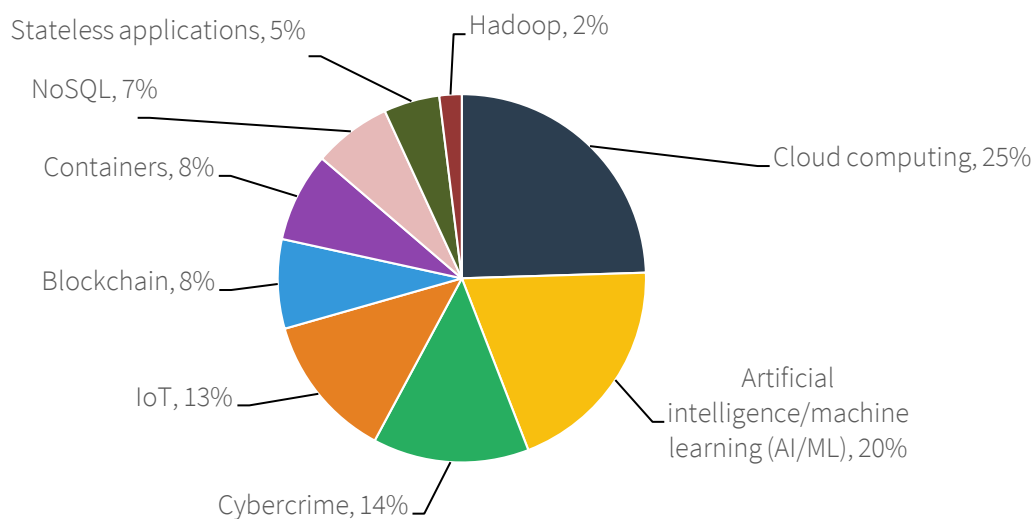
Cloud has brought about a lot of change in production patterns, with a quarter of survey respondents seeing cloud computing as the trend that will be *most disruptive* to their data protection strategies (see Figure 2).³ Just like with any innovation in IT that affects workloads, data protection best practices updates and new opportunities to protect data emerge.

² Source: ESG Master Survey Results, [Data Protection Cloud Strategies](#), June 2019.

³ Source: ESG Master Survey Results, [2018 Data Protection Landscape Survey](#), November 2018.

Figure 2. Cloud Will Disrupt Data Protection Strategies

Which of the following technology meta-trends do you expect to be the most disruptive to your organization's data protection strategy over the next three years? (Percent of respondents, N=320)



Source: Enterprise Strategy Group

Disruption is not necessarily a negative force: 87% of organizations report that cloud computing has become an important part of their data protection strategy that has enabled them to better and/or more efficiently protect their data. However, challenges such as security/privacy and data loss (recovery point) concerns persist.⁴

One of the cloud services that organizations are turning to as part of their strategy is the well-known brand Google, with its Google Cloud Platform (GCP). As applications, data, and services are increasingly consumed on GCP, backing up and recovering data can be significantly simplified with the “cloud-native” purpose-built HYCU solution.

HYCU for Google Cloud Platform

GCP offers failover and redundancy, which may lead customers to conclude that backup is automatically included. This is not the case. End-users are *always* responsible for managing their data and its protection. In order to apply backup and recovery best practices, enterprises can leverage HYCU's backup as a service solution.

The solution is a fully managed backup and recovery as a service with a simple subscription right from the GCP Marketplace. Customers don't have to worry about managing deployment of the software (there are no agents). It offers one-click VM and application backup, plus one-click launch. It also fully integrates into Google Identity Access Management (IAM) and works via Google Cloud API.

HYCU for GCP has unique design characteristics:

- **Native:** It uses native snapshots, integration with Google IAM, and Google storage buckets for optimal TCO. It does not require legacy backup agents.

⁴ Source: ESG Master Survey Results, [Data Protection Cloud Strategies](#), June 2019.

- **Delivered as a service:** This simplifies deployment at scale and grows as you go with an easy and modern set of management capabilities. Customers do not need to stand up virtual appliances or agents.
- **Easy to consume:** Billing for the backup service is fully integrated into Google billing.
- **Easy to scale:** HYCU was designed as a cloud-native application and can dynamically scale with the customers' environment. In addition, because of Google IAM integration, self-service recovery is easy to accomplish.
- **Focused on application protection:** HYCU can ensure applications are consistently backed-up and recovered.

HYCU will keep expanding capabilities in GCP in the coming months and is more broadly executing on a multi-cloud strategy through unified management. The company recently introduced HYCU Protégé to specifically address multi-cloud data protection by unifying data protection “under one roof” to help end-users leverage simplified capabilities to “lift and shift” their applications from one on-premises or cloud primary location to another and ensure data protection through the process. In addition, this new console provides a mechanism for customers to recover specific applications running on-premises onto Google Cloud for test and dev as well as a cost-effective disaster recovery option across clouds.

The Bigger Truth

Applications are moving to the cloud at an accelerated pace, which means their associated data sets must also meet compliance and data protection requirements. The adoption of Google Cloud Platform by many organizations as their primary cloud partner or as part of a multi-cloud strategy adds a new platform to protect to the enterprise backup equation.

While approaches exist to leverage legacy backup and recovery constructs, HYCU offers an interesting alternative to simply adding a GCP agent to your legacy environment with a native, purpose-built, and fully managed backup-as-a-service offering for GCP. The as-a-service technology that leverages the GCP platform fosters simplicity for the user with automation and focuses on recoverability.

This is a departure from traditional or legacy approaches centered around a core engine that leverages agents or integrations to retrofit applications or platforms into the solution's schema. While HYCU recognizes the need for unified management of multi-cloud environments for data protection purposes (Protégé), the company's approach is to go “deep” with one platform through extensive integrations, as it has successfully demonstrated with Nutanix and now with GCP.

ESG will keep a close eye on HYCU in this space and encourages users to take a close look at this service when evaluating the protection of their GCP environment. (Interested parties can simply click the trial option directly from the Google Marketplace.)

As HYCU adds customers to its growing list, we expect to hear from users about gains in operational efficiency, since the solution handles all aspects of deployment and maintenance in a “Google admin-friendly” fashion, as well as about the solution's fit for delivering enterprise-class data protection SLAs at scale.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.



Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

© 2019 by The Enterprise Strategy Group, Inc. All Rights Reserved.

