HYCU®

eBOOK

Why Backup as a Service Is a Key Part of Any Hybrid Cloud Environment

MSPs that bring a strong data protection perspective and expertise with Backup as a Service (BaaS) solutions have an opportunity to stand out from the crowd to win more (and bigger) deals.

Intro

As an MSP dedicated to helping organizations modernize their infrastructures and take advantage of the agility and cost savings of the cloud, you understand the importance of smart data management strategies. But, in the flight to the cloud, have you and your hybrid cloud customers stayed diligent with modernizing data protection strategies as well? Or are legacy backup and recovery tools jeopardizing your customers' strategic goals and putting data at risk?

In the last few years, cloud adoption took off at an unprecedented rate. Thanks in large part to the COVID-19 pandemic and the rise of remote work, organizations have rapidly modernized their IT infrastructure to minimize the cumbersome management of traditional data centers.

MSPs have played a key role, providing expertise to organizations that might not have the resources or knowledge otherwise. As a result, 92% of organizations have or are planning a multi-cloud strategy, while 82% of large enterprises have adopted a hybrid cloud infrastructure—which brings together on-premises, private and public clouds into one work environment.

While companies work hard to transition to the cloud, any of them who have been in business for more than a few years probably have on-premises infrastructure and legacy applications to include in their IT strategy. Even if a hybrid cloud environment is only a temporary stage for some until they migrate everything to the cloud(s), many organizations enjoy the benefits of hybrid cloud.

With a hybrid cloud model, IT teams can gain the benefits of agility, scalability, and cost-savings from public clouds for their organization. At the same time, they can maintain control over their critical workloads on-premises to keep a clear data ownership chain of command, which is particularly important in highly regulated industries like banking, financial services, healthcare, and government.

As an MSP that's helping established organizations modernize on-premises data centers with cloud storage and computing, not only do you need to help them streamline their production environment, but you also to need bring their backup and recovery infrastructure along with it.

Learn more about HYCU's MSP Program and how we can enhance your managed services portfolio here.

HYCU®

Backup and recovery solutions are critical tools in any organization's kit to manage and safeguard their data and applications from human error, cyber threats, and disaster. But in hybrid cloud environments, backup and recovery often becomes more complex—and, thus, introduces more complications for you as an MSP and more risk to your customers. MSPs that bring a strong data protection perspective and expertise with Backup as a Service (BaaS) solutions have an opportunity to stand out from the crowd to win more (and bigger) deals.

In this eBook, we'll explore the unique challenges of protecting data in a hybrid cloud model, the role an effective BaaS solution can play in an MSP's data protection strategy, and key considerations when recommending and implementing BaaS to your customers.

Key Data Protection Challenges with Hybrid Cloud Models

For all its virtues, hybrid cloud IT environments introduce a new level of complexity into application and data management. Managing these hybrid environments is a new skillset unto itself, and many MSPs are helping their customers address key data protection challenges, including:

01 Eliminating Silos

The biggest challenge of managing hybrid cloud environments is having to use disparate data protection solutions (including agents on-prem), which can add time, resource, and labor costs for the MSP and the customer. What's needed is solution that protects data anywhere with a single pain of glass.

02 Protecting the data protection infrastructure itself:

The real risk here is protecting the data protection infrastructure, encrypting data, managing access and permissions, on-prem and in the cloud.

03 Protecting multi-tenant clouds

These concerns are amplified for MSPs with multi-tenant clouds. The prospect of providing backup and recovery capabilities for hybrid cloud customers in this scenario can seem daunting, from orchestrating the data to ensuring the security and sovereignty of the data—all while doing it in a cost-effective way.

04 Protecting cloud workloads

When it comes to protecting hybrid cloud environments, skill and technology gaps are not the only hurdle to overcome. There's also the misperception that, for the cloud portion of the environment, that the native resiliency and availability of public cloud providers like AWS, Google, and Microsoft provide enough data protection.

Thus, your customers might maintain legacy backup and recovery tools for their on-prem software, while mistakenly underestimating the risk to their cloud workloads in doing so.

The shared responsibility model between cloud service providers and customers indicates that it is the CSP's responsibility to secure the infrastructure, but it is the responsibility of customer to backup and secure the data and applications running on that infrastructure.

The two options customers have is to manage this themselves and create their own snapshots and managing via scripts with limited visibility, which is time-intensive, or they can create agent-based legacy solutions that are not SaaS and add high resource and labor requirements to maintain.

Ultimately, hybrid clouds are delivering massive value to companies. But, when data protection is at stake, it's critical to acknowledge that hybrid cloud environments add a level of complexity that creates more opportunities for human error and cybercriminals to jeopardize the data and infrastructure of your clients.

How can you help close the data protection gap for your customers? **Read on to learn more.**

How to Approach Data Protection in a Hybrid Cloud Environment.

Any data protection strategy should act as a safeguard against the challenges of operating a hybrid cloud, while also complementing the value the hybrid cloud brings to an organization. The solution you choose should work together with that strategy.

When evaluating solution options, you want to bring the benefits of a modern hybrid cloud production environment to the backup environment. That means finding a backup and recovery solution that leverages the cost-savings of the public cloud and allows you to pay as you go. The ability to move away from maintaining secondary redundant sites and to paying for storage and compute as needed is critical.

There are many ways to approach backup and disaster recovery for a hybrid cloud environment, from using legacy on-premises storage to hardware appliances and virtual appliances to full-fledged BaaS. Though they may all provide a certain level of data protection, the day-to-day experience with each can be very different.

Ideally, the backup and data recovery tools you evaluate and provide for your customers should provide the same level of control and agility over backup environments as you have over your production environments.

Five things to consider:

1. Migrating from on-premises to the cloud isn't easy and can introduce scaling, downtime and data loss challenges.
2. Backup administration through legacy, on-prem infrastructure is more cumbersome than the production environment, especially for cloud-native workloads. Relying on agents to manage VM backups and clunky, retrofitted point solutions, sap the agility and time savings of a hybrid cloud environment.
3. It is difficult to meet key SLAs like Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) or get visibility into the backup and recovery preparedness of the entire hybrid cloud environment.
4. Recovery capabilities are not consistent across the different workloads.
5. Ransomware resiliency is not always factored into consideration, leaving companies unprepared to respond rapidly to ransomware attacks.

Learn more about HYCU's MSP Program and how we can enhance your managed services portfolio here.

Many companies and MSPs are evaluating the role a BaaS solution can play in their data protection strategy.

These solutions offer much of the value commonly associated with other SaaS providers—no upfront capital expenses, little-to-no resources needed to manage it, cost scales to your needs, etc. But when it comes to making BaaS a part of your hybrid cloud data protection strategy, you might have questions about how they work together.

Let's take a closer look at how BaaS solutions are the best choice available to help protect a hybrid cloud environment and jump into the key questions you and your clients need to ask when evaluating BaaS solutions.

How Backup as a Service Solutions Work with Your Hybrid Cloud Environment

01 What is BaaS, exactly?

Broadly speaking, BaaS moves your backup, recovery, and sometimes migration, depending on the solution, from on-premises, IT-managed resources, or offsite tape/disk-based media into the cloud. BaaS greatly simplifies maintenance and management of your backups, oftentimes condensing it all down into a single dashboard experience, paid for through monthly or annual subscription payments.

How this all happens varies from solution to solutions, of course, but at the end of the day BaaS solves many of the business problems associated with operating in a hybrid cloud environment.

02 The Value of BaaS with Hybrid Cloud

BaaS brings a new level of convenience and affordability to backup administration. By offloading all the infrastructure, maintenance, and upgrades to a third-party, you're free to focus on the larger goals for your clients, while also being better equipped to safeguard against data loss and crippling ransomware attacks. Affordability goes hand-in-hand with the convenience of BaaS because not only are you saving on the up-front costs of hardware or managing multiple tools to cover the entire hybrid cloud environment, but you're also only paying for what you're using.

One of the main concerns for any hybrid cloud environment when it comes to BaaS is how it plays with the on-premises part of the workload. Many of your customers' key applications are likely still operating in their data center. Since BaaS is built to be cloud-native, on-premises workloads will be protected in the cloud, which brings a new level of resilience and cost-efficiency to your customers' data protection. (One important note: This may or may not work depending on your customer's industry's tolerance for sensitive data being stored in the cloud, though you shouldn't discount BaaS outright since different vendors handle data control and security differently.)

If security is your key concern, BaaS can be a great way to augment your backup security. Most BaaS vendors provide the latest encryption standards to data in transit and at rest. Plus, key integrations with your identity management and access solutions simplify your backup security and bring it in line with your production environment's security standards. With air-gapped, immutable backups and affordable data storage, you'll also have a way to make a broader part of your infrastructure ransomware resilient.

Where BaaS really shines is handling the dynamic environment of cloud and hybrid cloud environments. Not only is data more portable between on-prem to the cloud and within the cloud, but you're able to expand and contract your workloads as your customers' business needs demand. And with BaaS, it's easier to bring new workloads into the mix from within the same or other clouds.

Lastly, your BaaS solution should make your data protection efforts for customers more efficient. Many BaaS solutions will be able to help you manage the challenges of migrating to the cloud. Even though migration isn't in the name, BaaS solutions can help you to quickly spin up dev instances and backups into new locations. Where some may fall short, however, is in moving from the cloud back to on-premises.

With all that in mind, how do you go about choosing the right BaaS solution to simplify the protection of your clients' hybrid cloud environment? **Let's look at key considerations to help you and your clients evaluate BaaS vendors.**

12 Key Things to Consider When Choosing a BaaS Solution

01 Does the BaaS solution support and align with the digital transformation goals that are driving your hybrid cloud adoption?

BaaS should support your drive for speed and agility in the cloud by simplifying your backup administration. It should also help you unify your backup administration, discover applications, and provide consistent protection across your environment.

02 Is the solution designed to be cloud-native and integrate deeply with your chosen cloud service providers?

Some BaaS solutions may be slow to update alongside your cloud service providers, especially as new cloud data center regions open. Your BaaS solution should not require updates or maintenance to work alongside your CSP.

03 If you're relying on your legacy infrastructure for backups, what resources will BaaS free up?

As part of your data protection strategy, BaaS can reduce your reliance on legacy, on-premises infrastructure and appliances. Calculate the cost savings in both upfront capital expenses needed for backup and time saved maintaining the infrastructure on your own.

04 What are the key SLAs for your backup and recovery strategy and how will BaaS help you improve them?

BaaS will make it simpler to backup and recover more of your data and applications than ever before. Depending on your network capabilities and your BaaS vendor, it will impact your RPO and RTO. Ideally, your BaaS vendor should help you meet these SLAs without impacting your production environment.

05 How long will it take you to deploy and configure the BaaS solution before you can protect your applications and VMs? Will you need to deploy and maintain agents to backup VMs?

BaaS should eliminate the need for deployment and minimize configuration needed to start protecting your cloud-based workloads. For your customers' on-prem workloads, BaaS solutions should provide a big improvement over the cumbersome deployment and configuration of legacy tools, removing the need for manual installs that drag out the deployment process for days and weeks and require constant sizing exercises.

The need for locally installed agents or plugins for your VMs will slow down your backup and recovery process, mitigating the resource and cost savings potential of BaaS solutions.

06 How much time and effort does it take to size and scale your backups to match your production environment?

Ideally, your BaaS solution will take little to no effort as it scales alongside the production environment. Whether your customers' infrastructure footprint is expanding or contracting, the BaaS solution should help you optimize and automate backups, including automated application discovery.

07 How simple, fast, and granular is the recovery process?

Granular recovery doesn't always align with "fast and simple," whether you're talking about traditional backup solutions or BaaS. With a BaaS solution that's cloud-native and integrated deeply into your cloud platform(s), fast, simple, and granular backups are possible with agentless architecture. When you're administering backups and recovery across your workloads through a single user interface, you've got an added benefit of determining your best recovery target as the situation demands.

08 What is the process like for migrating and recovering data from the cloud to your on-premises solution?

Running a hybrid cloud means you'll need to shift data from cloud to on-premises and vice versa. While most BaaS solutions can easily handle on-prem-to-cloud migration, the reverse is not always the case.

09 What level of training and day-to-day involvement is required for your backup administrators to keep everything running well?

Your BaaS solution should have an intuitive, familiar user interface that helps unify and simplify managing the backups across the hybrid cloud environment. Your solution should be light weight, nimble with less moving parts and provide detailed logging mechanisms that can facilitate instant upgrades, minimal maintenance, and include outstanding customer support—ensuring you or your customers can make the complexities of backup and recovery effortless.

10 How will BaaS support your growing need for ransomware protection and resiliency?

Ransomware recovery is not simply disaster recovery. You need a BaaS solution that can protect your customers' data through air-gapped, immutable backups and enable rapid recovery of your infrastructure with application-consistent backups. This will allow you to get your clients back to business quickly and avoid costly downtime.

11 How does the BaaS provider support multi-tenant environments?

Your chosen BaaS solution should be designed to isolate the application state and data model for each of your customers, giving you a logical separation model for each customer and preserving their unique security and privacy model while maintaining the efficiency and scalability of the cloud.

12 Do you/your client retain sovereignty over the data?

Some BaaS providers use a private cloud deployed within a public cloud environment, meaning they take control of the data in the process of backing it up. This adds another layer of risk, and for those subject to privacy regulations like the EU's Global Data Protection Regulation, it may make it impossible to back up some data with BaaS vendors. Your chosen BaaS vendor should ensure total data sovereignty and control to simplify yours and your customer's life.

Is BaaS the Right Move for You and Your Customers?

Hybrid cloud data protection is a critical, but underserved, area of digital transformation. Service providers can adopt a BaaS solution that can complement the modernization and cost-saving efforts of their customers.

Not all BaaS vendors are created equally, however. As BaaS is a relatively new subset of backup and recovery solutions, the category is still evolving. We here at HYCU though believe our approach to BaaS will help companies with hybrid and multi-cloud environments tackle data protection securely, efficiently, and cost-effectively. For MSPs, we ensure they have the support they need to manage multi-tenant data protection, accessible reporting and automation, and greater visibility into your customers' data and applications.

HYCU Protégé is a cloud-native BaaS solution designed to simplify multi-cloud and hybrid cloud data protection, migration, and disaster recovery. Our platform begins with purpose-built, native solutions for each of the supported public cloud, private cloud, SaaS app, and databases. No clunky, retrofitted point solutions here.

This helps you provide the best data protection and recovery capabilities no matter the unique configuration of your customers' hybrid cloud.

With HYCU as your BaaS provider, you're also helping to futureproof data protection offering for your customers. No matter how your customers' hybrid cloud environment evolves over time, you've got a partner that can help you protect and recover it all.

Learn more about HYCU's MSP Program and how we can enhance your managed services portfolio here.

109 State Street, Boston MA 02109, USA | Phone: +1 617 681 9100 | E-mail: Info@hycu.com |

Copyright © 2022

《 BACK