HYCU®

FUTURE-PROOFING YOUR BACKUP AND RECOVERY STRATEGY

Why Backup as a Service Is Fundamental to Multi-Cloud Environments

START 》

INTRODUCTION

The right backup and recovery strategy will provide IT organizations with the control they need to pair with the speed and agility of their cloud-driven workloads today—and tomorrow.

IT teams and environments have undergone a tectonic shift the last ten years, a shift only accelerated by the COVID-19 pandemic. Few developments have been more consequential than the move to the public cloud. Back in 2012, three new Infrastructure as a Service solutions arrived to challenge Amazon Web Services: Google Compute Engine, the now-defunct HP Cloud, and Microsoft Windows Azure. The nascent cloud wars kicked off a rush to move workloads from on-premises to the cloud to take advantage of the cost savings and agility.

Over the last ten years, IT teams have been building the proverbial airplane of a modern IT environment. All the while, they've had to oversee the exponential growth of data and applications, which is sort of like trying to fly the plane while building it. Not for nothing, IT teams are already looking toward the future with edge computing, automation, artificial intelligence, and widespread IoT adoption, which is like outfitting that plane for space travel at the same time.

Suffice it to say, IT teams have a lot going on. The data that runs through the IT organization's infrastructure is helping power rapid growth and deeper insights for key business units. Building an agile, secure, reliable environment that will stay that way for years to come is critical to the overall health of the business.

Unfortunately, many IT teams are languishing in the here-and-now. According to Deloitte, 55% of IT teams spend over half the budget simply on maintaining business operations, while 19% of that is spent building new capabilities. The shift towards cloud-native platforms and as-a-service solutions should help move that balance towards innovation, with the companies on the cutting edge aiming for parity between operations and innovation spend in the next 3-5 years.

As CIOs and IT directors look to invest in a modern, agile IT infrastructure that is less a cost-center and more of an investment for growth, they'll need to ensure that they can also deliver control and security alongside speed and agility. A modern approach to backup and recovery through Backup as a Service (BaaS) is the perfect complement to the cloud-native, application-driven IT organization.

In this eBook, we're going to focus on two key points companies need to consider as they modernize their IT infrastructure: the big data protection challenges that will keep IT teams busy for the next few years, plus developing a backup and recovery strategy that is designed to support the evolution of your IT organization as it moves into the cloud and beyond.

DATA PROTECTION CHALLENGES OF TODAY AND TOMORROW

All the exciting changes in the IT world have not been without their counterbalancing forces. At the heart of these challenges lies the issue of control. With the move to the cloud (and as-a-service offerings more broadly), IT teams have traded simplicity and speed for total control over their infrastructure. That's why data protection is more important than ever.

Today, data protection is about more than creating copies. Data protection should be how you deliver a sense of control to your IT organization. Modern data protection means backing up, migrating, and recovering your data, VMs, and other resources securely, with the same speed and agility expect of your production environment.

With your modern data protection strategy, you'll be able to tackle the challenges that will shape your IT organization over the next few years. Let's look at the five most pressing challenges relying on a future-proofed data protection strategy.

1. Consumers and lawmakers are tuned in to data privacy

High-profile consumer data breaches at companies like Yahoo, Facebook, and Experian put data protection in the public eye. Consumers are more aware than ever of how much data companies are collecting and how that data is being used. When surveyed by KPMG, 86% of consumers feel a growing concern about data privacy.

That, in turn, has led lawmakers across the globe to grant sweeping protections to consumers over their data. Laws like the EU's General Data Protection Regulation and the California Consumer Privacy Act are setting the bar for corporate data responsibility.

Companies that are lackadaisical about data protection will feel the impact on their brand reputation and in their wallets.

2. Cyber criminals are more prolific and savvier

In 2021, ransomware attacks increased 105% globally, while governments (1,885% increase) and healthcare (755% increase) were hit especially hard. It's estimated that in 2021 there was a ransomware attack every 11 seconds.

Cyber criminals have realized that compromising your data and infrastructure is a worthwhile endeavor, because the threat of being knocked offline for weeks and months makes companies willing to pay hefty ransoms. As companies ramp up detection and protection efforts, the rise of ransomware also means companies need to evaluate their data protection strategy for ransomware readiness.

If the trends continue apace, cyber threats are only going to grow in the future, making ransomware readiness a key component of any future-oriented strategy.

3. Multi-cloud and hybrid cloud fragmentation creates silos

The move to the cloud is not without its challenges. Companies with workloads spread across multiple clouds or between public clouds and on-premises/private clouds are moving fast, and that can introduce new risks.

With more moving parts, companies need to ensure they're not creating new silos. The ease of spinning up new VMs or moving data to cheap public cloud storage can mean proper security measures aren't being enforced or critical maintenance and updates are being missed. This can create more opportunities for bad actors to gain a foothold.

4. The nature of work has changed forever

The remote work trend was jumpstarted by the pandemic closing offices worldwide. After two years, the trend is holding, with nearly 60% of workers whose jobs can be done from home continuing to work remotely, according to Pew Research.

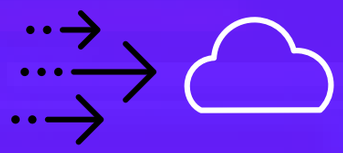
The shift to remote and hybrid work further accelerated the move towards the cloud, but it has also introduced concerns about data privacy and security. IT and security teams must incorporate this new wrinkle into their education and risk management, as well as ensuring that data is safe wherever it's being generated and used.

5. Precious IT resources will be stretched thin

Whether its employee burnout, shrinking budgets, or worker shortages, IT teams like many others are facing a future with an uncertain set of human and capital resources. All the while, IT orgs are expected to do more to move the business forward with a modern architecture.

Protecting your data should be neither an afterthought in your IT strategy nor a burden that prevents you from innovating. Advances in as-a-service solutions for backup and recovery help ease the load on your IT teams by simplifying the backend of your backup infrastructure to a third-party.

With these challenges in mind, let's evaluate the three key goals of a data protection strategy that will help you build towards the future and safeguard your company along the way, as well as the steps you



BACKUP AND RECOVERY FOR TODAY AND THE FUTURE OF IT

Goals for Future-Proofing Your Data Protection Strategy

Your data protection strategy doesn't have to be complicated to be future-proofed. There are three key goals to keep in mind when aligning your data protection strategy and your IT goals today, and into the future.

THE SAFETY OF YOUR DATA

Back in the 80s, American television featured a stark public service announcement that asked parents, “It’s 10 p.m., do you know where your children are?” When it comes to the safety of your data, you should be asking the same question: where is it all and is it secure?

As corporate data grows exponentially over the next few years, your data protection strategy should focus on the safety of the data. Safety, in this case, is a combination of both security—managing access, establishing protocols—and control—the ability to do what you need to with your data without prohibition. With more business units creating more data and utilizing cloud-native applications or platforms, IT teams will find themselves struggling to manage both sides of the safety coin effectively.

A unified approach to data protection, including a single view of all your data, VMs, and other resources within your backup and recovery environment will be critical for safeguarding data. IT teams will need everything from air-gapped, immutable backups to strong identity and access management to visibility and ownership over your data to help maintain the agility and resiliency of production workloads without sacrificing data safety.

MULTI-CLOUD AND HYBRID ARCHITECTURE

Public clouds are responsible for the modern IT environment but getting there isn't as simple as choosing one cloud platform and calling it a day. Create a data protection strategy that aligns with a business that will operate on multiple clouds to help keep yourself agile in the future.

IT teams work in multiple clouds for a variety of reasons. Maybe you're avoiding vendor lock-in by utilizing competing public clouds for your various computing and storage needs. Maybe different business units rely on another cloud. Maybe mergers and acquisitions necessitate a move to another cloud.

The future of your cloud environment is not set in stone... it is, appropriately, always up in the air. Your data protection strategy should be built on this premise and support a wide array of cloud platforms. Cloud-native architecture, deep integrations, and roadmap alignment with the cloud platform is also important.

DATA MOBILITY AND RECOVERABILITY

The third goal of your data protection strategy should focus on securing your data beyond simple copies and individual files. Whether you're running a multi-cloud or hybrid cloud architecture, the mobility and recoverability of your all your data or data assets will help you stay agile and resilient for the future.

Shifting workloads, spinning up VM clones, and ransomware are all made easier with a data protection strategy that prioritizes mobility and recoverability. Your backup and recovery technology should enable you to dynamically move and restore from cloud to cloud or back to on-premises with ease.

WHAT SHOULD YOU DO TO PREPARE?

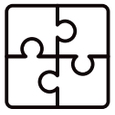
What should a forward-looking IT team be doing today to create future-proof backup and recovery capabilities that support the broader data protection goals? There are six key things you should be considering right now to set yourself up for success in the future.

1. Get comfortable with the public cloud

For all the oft-discussed virtues of the public cloud, there are still misconceptions and apprehension around it. Understand the reality of the public cloud first to make sure you're building towards a cloud-ready backup and recovery strategy that works seamlessly with your chosen cloud.

Public clouds are not inherently less secure than your on-premises infrastructure. They're built with security in mind and bear shared responsibility for your data. Know the limits of a cloud platform's responsibility and exercise proper encryption and identity and access management. It's possible to take advantage of the public cloud without sacrificing data protection and can even help global companies comply with data privacy laws that limit where consumer data can be stored.

On the opposite end of the spectrum, don't rely too heavily on the backup and recovery capabilities of the public cloud providers. Snapshots, for instance, aren't a viable substitute for backup and recovery on their own. They become too cumbersome and expensive to manage for most organizations.



2. Create policies that won't get lost in translation

Technology without process is a surefire way to waste resources. Your backup and recovery solution should be guided by policies aligned with business requirements.

Before choosing a new backup and recovery solution, be sure to gather and understand the business requirements it will be supporting. Business stakeholders and technology stakeholders need simple, mutually agreed upon measures. Whatever technology you end up with should be able to take these measures as inputs to create clear, actionable policies.

3. Eliminate sizing exercises

There's no room for sizing exercises in the future. Sizing exercises shouldn't be painful, nor educated guesses, but that's what they inevitably become. No matter how well planned your future is, you'll always be wrong when it comes to sizing your backup requirements.

Don't assume sizing exercises are the cost of managing backups. You need a backup and recovery solution that can scale-up and scale-out with ease. Removing the burden of sizing exercises will free up key resources to focus on more innovative tasks.

4. Build with a set-and-forget mentality

A dynamic and agile production environment will grind to a halt as soon as it hits the backup environment if your solution isn't automatically tracking for new applications, VMs, or databases. Protecting your newly provisioned resources should happen without you thinking about it. And your maintenance and updates should be similarly hands-free. That's the only way you'll deliver a data protection strategy that aligns with the values of your production environment.

5. Prioritize ransomware-ready disaster recovery

The threat of ransomware can't be solved with traditional disaster recovery. Whereas you might normally recover the most recent iteration of your production environment, with ransomware you'll need to recover to before when the attack happened. In some cases, ransomware sits dormant for months.

The threat of ransomware should also shift how you think about backups. You'll need to create immutable backups that are segmented from your primary network. And you'll need to protect all your data with application-consistent backups so that you're recovering to a business-ready state in minutes and hours, not weeks and months.

6. Aim for cost-efficient protection technologies and strategies

With all the above, it's important to recognize that you're probably asking more of your backup and recovery strategy than ever before. And you probably aren't getting a huge budget increase for it. Do you have the infrastructure, licenses, and storage to do it all?

Backup and recovery solutions delivered as-a-service will greatly reduce your capital expenses for data protection, which will in turn free up money for innovation and simplify life for your backup administrators.

EVALUATING BACKUP AS A SERVICE AS PART OF YOUR FUTURE STRATEGY

Companies will take many different roads to arrive at a modern, cloud-driven IT organization.

Like most parts of your business, as-a-service technologies will play a key part in the future of your data protection. Backup as a Service moves your traditional on-premises, IT-managed backup infrastructure to the cloud. By taking away the need to manage the backend, BaaS frees up resources and allow you to focus on creating a more unified, simple approach to data protection. locally and replicated to alternate locations.

Finding the right BaaS vendor will depend on your current (and future) workloads and how the vendor's technology manages backup and recovery since there is no standardized way for BaaS to work.

Before talking to a BaaS vendor, understand your business goals and the roadmap of your IT architecture for the future. You'll want to make sure that the vendor not only supports your key goals—such as becoming ransomware-ready and improving key SLAs—but that the vendor also is aligned with your chosen cloud service providers. Poor alignment between a BaaS solution and a public cloud platform can cost you. For example, when providers open new data center regions, you might be waiting months to take advantage of the new capabilities and cheaper storage before you're able to move.

When evaluating a BaaS solution, you can't evaluate it against the same standards as legacy backup and recovery solutions. That's because the simplicity, automation, and dynamic nature of BaaS unlocks new use cases for your multi or hybrid cloud architecture—just like your cloud-native workloads unlocked new possibilities compared to your on-premises workloads.

Most importantly, you want to find a BaaS provider that will be a trusted partner throughout your IT modernization. BaaS solutions should give you more control than ever while simplifying the tedious and costly elements of backup administration like maintenance, updates, and sizing exercises.

To make sure your IT organization's future is headed in the right direction—to the cloud, edge, and beyond—make sure you have the right backup and recovery strategy in place to support it.

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