**Unitrends Backup, Recovery and Continuity**
White Paper

# 7 Ways to Improve Backup, Recovery, and Continuity

## It's Time for Radical Improvements

**Unitrends Backup,**
**Recovery and Continuity**
White Paper

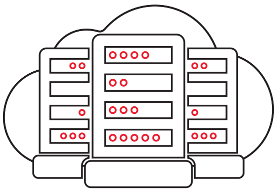
# 7 Ways to Improve Backup, Recovery, and Continuity

It's Time for Radical Improvements

## Backup and disaster recovery need to improve. Not incrementally: radically

Most enterprises run backup tools and processes designed for older platforms and simpler times: before hyperscale clouds, near-ubiquitous virtualized workloads, or SaaS applications. Many still use solutions that rely on tape for retaining data. These systems are inefficient, costly, and difficult to manage. They can't scale to serve exponential data growth. They don't respond well to new threats. They make it more difficult to execute on digital transformation or other strategic initiatives. Worst of all, you can't confidently rely on them during a disaster.

Fortunately, you no longer have to live with these problems. Backup technologies and best practices have improved dramatically in recent years. Now, you can transform backup from a low-level legacy IT function to a modern enabler of business continuity and value. This white paper outlines 7 practical, actionable steps you can take today. By focusing on them, you can establish disaster recovery systems that support any technology or business strategy — and always work when you need them most.

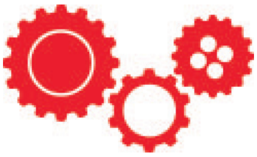


## 1. Consolidate multiple backup solutions onto one platform

As IT environments have become increasingly complex, many organizations have turned to multiple point solutions for backup and recovery. They usually had good reasons for deploying these tactical solutions, and often had little choice: conventional enterprise backup solutions weren't technically capable of backing up their rapidly-evolving portfolios of systems and data.

Today, enterprises may have separate backup systems for physical Windows and Linux servers; legacy UNIX hardware; virtualized workloads; data and systems operating on public hyperclouds such as Amazon Web Services or Microsoft Azure; and even individual SaaS platforms such as Microsoft Office 365. But this non-integrated backup infrastructure is costly and difficult to manage.

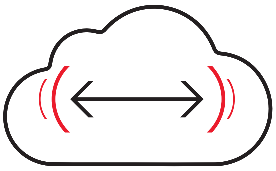
Fortunately, you can now consolidate these backup workloads onto a single platform with a unified interface. You'll need to maintain fewer licenses, maintenance, and service agreements. You can reduce training investments, and gain staffing flexibility: any administrator familiar with the unified interface can step in and handle backup for virtually any system. You can choose new platforms and suppliers without having to rip out backup systems. And you can hold a single vendor accountable for the performance of all continuity systems.



## 2. Automate, automate, automate

Forward-looking IT organizations have recognized the critical importance of automation in continually providing new services, supporting new users, and meeting new requirements. They have moved to automate tasks ranging from spinning up VMs and deploying cloud apps to performing software builds. But few have taken full advantage of the many opportunities now available to automate backup and recovery.

Today, you can automate not only core scheduled backup processes, but also processes associated with moving backup data offsite to the cloud. This means you can rapidly move most backup tasks away from manual processes involving tapes, rotational media, and physical shipping. You can also automate comprehensive reporting about your backups. Most important of all — as we'll discuss in greater depth in Item #4 — you can also systematically automate backup and disaster recovery testing, thereby gaining unprecedented confidence that your backups will work.

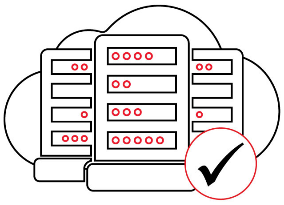


## 3. Leverage cloud elasticity and economics of scale

Cloud services are transforming the way IT organizations build, manage, deploy, expand, and shut down applications. Backup and disaster recovery are perfectly suited for the flexibility and elasticity that the cloud makes available. It's time to take advantage of this.

By building cloud capabilities into your backup and disaster recovery toolset, you can smoothly address explosive data growth. Instead of continually buying large quantities of costly on-premises storage to back up local workloads, rely on just-in-time availability of cloud storage, and cloud providers' remarkable economies of scale. Cloud-integrated backup may also make it easier to provide the physical isolation you need to protect against ransomware. Cloud-based backup can also be used as the basis for DR as a Service (DRaaS) to quickly recover workloads using cloud compute resources in the event of the disaster.

Best practices exist to quickly and efficiently move data between your premises and cloud storage. You may (or soon will) possess hundreds of terabytes of data: more than can easily be transferred via WAN. Therefore, you can start by "seeding" cloud storage: physically delivering rotational media with up-to-date data. After that, you can automate uploads of new and changed data, optimizing transfers with compression and advanced deduplication. Cloud-connected appliances can provide fine-grained control over which data to upload to your cloud provider, and which business-critical backups must always stay on premises for near-instant recovery. To protect network performance, you can throttle bandwidth up or down based on the hour of day, or other network traffic.



## 4. Test recovery assurance systematically, continually, and automatically

IT organizations have struggled with backup and DR testing for years, and traditional solutions offered little help. Testing has usually been a laborious manual process, and it sometimes disrupted end users. Given this, many organizations tested their backups rarely, if at all. Or they might test the integrity of backup data, but not their ability to quickly recover complex applications. As enterprise systems have incorporated even more dependencies, these problems have worsened. Fortunately, they can now be solved through automation.

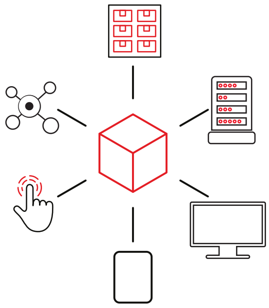
> Using new recovery assurance tools, you can automate testing of even the most complex backup environments.

Using new recovery assurance tools, you can automate testing of even the most complex backup environments. You can now define Recovery Point Objective (RPO) and Recover Time Objective (RTO) performance targets on a per application basis, and then configure your tool to test each app as often as needed: monthly, weekly, or even daily.

Automated tools can now spin up and validate workloads within your offsite disaster recovery environment, using backups stored there. They can test complex n-tier applications to ensure that all interfaces and configurations are working properly, and nothing has drifted out of compliance. They can handle complex boot order sequences, including presentation tier, web server, business logic, and database. They can test network routing rules and third-party API calls.

You get a timely report certifying that your disaster recovery point will work exactly as expected. If problems are found, they can be pinpointed and solved now — not under the pressure of a disaster.

Automated testing is one key reason you can now demand more rigorous recovery time standards, including true guarantees, not just “best effort” promises.

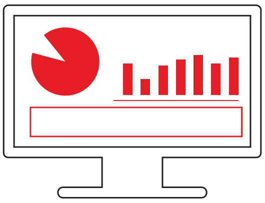


## 5. Improve flexibility

In today’s era of digital and cloud transformation, your environment changes faster and more continually than ever before. Recognizing this, IT organizations seek to maximize their flexibility in all areas. Backup and continuity should be no exception.

Traditional enterprise backup solutions have been obstacles to change, failing to support new platforms or approaches to service delivery. Many were originally architected to solve only a single problem, such as backing up virtual machines.

Make sure your solution will adapt as you evolve: don’t lock yourself into one architecture or approach. Consider the following scenario: You want to quickly leverage the economics of cloud-enabled backup now, but your major initiative to leverage Amazon Web Services or Microsoft Azure won’t start for 12-18 months. Choose a partner that offers a purpose-built backup cloud today, and will also support backup to your hyperscale cloud provider(s) of choice later. By doing so, you can also preserve the option of building hybrid clouds that leverage your own resources and those of multiple cloud providers, based on the value they offer in each application or environment.



## 6. Simplify via an intuitive user experience

For simple efficiency, you want a tool that simplifies and streamlines all backup and recovery tasks: both those that are performed routinely, and those that are performed only rarely. A modern, intuitive user experience is a priority: it should always be possible to operate your backup system without referring to a manual, and substitutes or managers should be able to do it when primary admins are unavailable. Easy user interfaces reduce costs for training, support, and fixing mistakes. (They also make day-to-day work just a bit more pleasant.)

But user experience is even more crucial during a disaster. By their nature, disaster recovery tools will be used in times of great stress. Operators must react quickly and accurately: they can’t afford to make mistakes that compound the disaster. Unfortunately, error rates typically soar when operators are under stress. Therefore, tools should actively guide users through the steps they need to follow, clearly explain what will happen when they do, and clearly explain what is taking place at every step of the process.

Great strides have been made in user experience over the past decade, as developers of consumer software have learned to streamline tasks, rely more on visuals and intuitive icons, and build more navigable interfaces. Not all enterprise backup/recovery systems reflect this consumer-driven innovation. Choose tools that do.

## 7. Protect all your assets

Finally, you want to be able to protect everything you have, and will have. That includes physical workloads, Windows, Linux, and legacy Unix servers, and all your virtualized platforms — often, not just VMware and Microsoft Hyper-V, but also Citrix XenServer, KVM or others. It means protecting not just individual private or public cloud systems, but complex OpenStack cloud environments controlling dynamically changing collections of compute, storage, and network resources. It means protecting SaaS applications such as Microsoft Office 365. And it means protecting all clients, since threats such as ransomware won't always be restricted to Windows.

As we've already said, protecting each type of system with its own point solution is increasingly untenable on grounds of cost and complexity. Increasingly, compliance is also an issue. So, for example, an SaaS or cloud provider might retain data for 90 days. But the government may require you to retain that data for seven years, and be capable of retrieving any of it quickly on demand.

You need a solution designed to support all of your platforms and business requirements, both current and emerging. Fortunately, such solutions now exist… which brings us to the final point we'd like to make.

## Discover Unitrends

At Unitrends, we've reimagined business continuity as a true solution: an opportunity to drive value, not merely a task to perform or an obstacle to overcome. Our Connected Continuity Platform™ capitalizes on cloud agility and economics to reduce your spend, tackle new threats, and help you gain 100% confidence in rapid recovery of all your data and systems.

We offer the industry's broadest portfolio of solutions for backup, cloud continuity, disaster recovery, and recovery assurance — and the industry's lowest total cost of ownership, too. Our solutions are radically easy to use, offer outstanding flexibility in any IT environment, and can fully protect any mix of physical and virtual assets, including 200+ versions of operating systems, applications, and hypervisors.

> At Unitrends, we've reimagined business continuity as a true solution. Our Connected Continuity Platform™ capitalizes on cloud agility and economics will help you gain 100% confidence in rapid recovery of all your data and systems.

Our Recovery Series physical appliances and Unitrends Enterprise Backup software provide local data backup and recovery for both physical and virtual environments. Integrated with our Unitrends Cloud backup and DRaaS solutions, they provide long-term data retention, so you needn't maintain a second disaster recovery site. Our Adaptive Deduplication software dramatically reduces storage requirements, and recovery assurance technology provided via our ReliableDR™ software orchestrates automated DR testing to provide you with 100% confidence in the recovery point to come. All of these are backed by a world-class, fanatically committed support team with a customer satisfaction rating exceeding 98 percent.

We'd welcome an opportunity to serve you. Visit unitrends.com to get free trial software, schedule a demo, or test drive an appliance. Discover how Unitrends can help you recover far more than just your data.