

# 5

## Tips to Simplify Your Data Protection

The security of knowing you can easily protect data across up to six hypervisor environments is available today.



In this digital world, there is an ever-increasing amount of data for you to manage — and that growth will only continue to accelerate. IDC's Digital Universe study states that enterprise data doubles every eighteen months. If this notion causes your chest to tighten or your stomach to get queasy, there is a good chance you are responsible for managing that data.

Many small- to medium-sized businesses (SMBs) are simultaneously running physical, virtual and cloud environments. With the widespread use of cloud technologies in recent years, companies began adopting a hybrid approach. The [IDC Cloudview 2016 Survey](#) revealed 68 percent of respondents use, or plan to use, a hybrid IT infrastructure. This is a seven percentage point increase over [2014 IDC Disaster Recovery Survey](#) stating 61 percent were using virtual technologies. The race to employ these technologies to keep ahead of the data, however, created some potholes in the road.

## As IT Environments Grow, Data Backup Becomes a Challenge

Today, more SMBs have transitioned to a hybrid environment, with 2016 estimates of virtualization at 76 percent according to [Spiceworks 2016 State of IT Report](#). With the amount of data generated by the average business continuing its fast growth, IT organizations embraced the hypervisor environment for better efficiencies and computing usage. Organizations with remote offices build environments that include, for example, Red Hat Virtualization, Linux KVM, and Citrix XenServer. Implementing different or additional hypervisors allows these organizations to lower costs.

## Avoiding the High Costs of Downtime

If your data is not secure and complete, this can cause data loss, downtime – or both. In a recent study from [Vertiv \(f/k/a: Emerson Network Power\)](#), unplanned recovery and data center downtime costs nearly \$9,000 per minute. Yes, per minute. One of the factors this study points to is the complexity of the IT infrastructure.

The modern backup environment has become disjointed and difficult to scale. This is due to silos of important company data and applications on old, physical servers, virtual hosts housing different virtual machines, applications and hypervisors, and the large number of virtual machines in the cloud for a company's IaaS cloud applications such as Amazon, Microsoft Azure and Office 365 and Google, to name a few.

In addition to the number of issues from natural disasters or internal user errors, today's IT and virtualization professionals also need to protect from new unforeseen external attacks such as ransomware. This is a painful type of malware that is illegally introduced onto your computer for malicious reasons. When ransomware infects your computer it blocks access to your data until you pay the criminals who are extorting you. According to Symantec's 2017 Internet Security Threat Report, 64 percent of Americans are willing to pay the criminals to get their files back, as opposed to only 34 percent of victims worldwide. And even then you might not get your data back. Symantec reports that just 47 percent of global victims who paid up got their files back.

**It's not good enough to just stop ransomware**, you need to detect it, deflect it, and restore the encrypted files if you want to survive the attack.

It may seem overwhelming to actively and completely protect all your important business data while addressing these challenges – and do so in multiple hypervisor environments. But it can be done. You just need to simplify your protection while improving your recovery time objectives (RTO) and recovery point objectives (RPO). How? Businesses need to think about how they are protecting their data across multiple locations and what data protection solutions will make sense for their future needs.

As you consider your new generation data protection in a multi-hypervisor environment, we wanted to share 5 tips to simplify your data protection and break through the complexity of multiple hypervisor environments.

# Simplifying data protection



## 5 tips for breaking through the complexity of multiple hypervisor environments

### 1 Simplifying in a Hybrid Environment

Select a solution that simplifies backup by offering a consistent look and feel across different hypervisors. This offers ease of use and gains better control and management of your critical data.



### 2 Complete Data Protection

Whether your data resides in physical, virtual servers, or Cloud (Azure, AWS, Private Cloud) ensuring complete data protection is vital. Choose a solution that can unify data backups across up to 6 hypervisors to simplify and future-proof your IT environment.



### 3 Speed and Flexibility Are Important

In the event of an unscheduled recovery, speed is critical to ensure business continuity. Be sure your solution offers portable workloads to simplify backup and restore a physical server, plus transfer between hypervisors and physical machines, easily and quickly.



### 4 Robust Integration

Reducing data loss is paramount for any business. Integration with your hypervisors ensures an efficient use of host resources when backing up physical, virtual, cloud, and mobile apps and storing data in different locations such as disk, tape or cloud.



### 5 Affordability

Ensuring efficient use of the physical infrastructure will minimize your hardware investment. Look for subscription licensing models to reduce balance sheet burdens by shifting capital expense (CAPEX) investments to operational expenses (OPEX).



## 1. Simplify Your Hybrid Environment

As outlined above, a cobbled together hybrid environment creates a level of complexity. You need to consider if your solution offers customizable dashboards that will provide immediate insights into the status of your environment to quickly resolve issues. Simplifying the backup process in this environment can be achieved by offering a consistent look and feel across different operating systems, or hypervisors. This gives you better control and management of your business' critical data, plus a unified interface reduces work and time for the system administrator by introducing ease-of-use.

## 2. Protect All Your Data

According to IDC, you should expect one unscheduled outage/recovery per year. This may not be just from big natural disasters or terrorist type of attacks, but are most likely from user errors and hardware failures. And, with the added business risk of ransomware becoming more prevalent, businesses need to be more proactive with their secure data protection. These types of unexpected outages are not only costly but if your data is not complete it could be risky for your business continuity. You need a solution that introduces simplicity to these complex environments without jeopardizing protection. Whether your data resides on physical or virtual servers, the cloud, or mobile apps, ensuring your business continuity is vital.

## 3. Get the Fastest and Most Flexible Solution

In the event of an unscheduled recovery, speed is critical. You need a solution that can recover in seconds or roll back in no time flat. Implementing a best-in-class solution that can handle these types of recovery times and institute instant restores, will reduce overall RTOs. Consider portable workloads that will allow you to backup and restore a physical server and transfer between hypervisors and physical machines easily and quickly when time is of the essence.

## 4. Aim for Robust Integration

Reducing data loss is paramount for any business. A robust integration with your hypervisor environment ensures an efficient use of host resources when backing up virtual machines and storing data in different locations such as a disk, tape, or cloud. This is essential in a multi-hypervisor environment. Selecting a solution that can unify data backups simply -- across up to six hypervisor environments -- is key to ensuring complete data protection.

## 5. Target Affordability

Hidden costs can put undue pressure on your budget -- and your IT department. Hypervisor server diversification is an important initiative in many organizations -- but don't fall into the trap of adding infrastructure costs and increased backup complexity in an effort to lower licensing costs. You want your data center to transparently migrate data from one hypervisor to another for efficient hypervisor recovery, which will help you avoid these hidden costs.

## Acronis Sets the Standard for Simplifying Hybrid Cloud Data Protection

Acronis Backup 12.5 is the world's easiest and fastest backup solution for your entire virtual environment, whether it is located on-premises, in remote systems, or in private or public clouds. It is the only backup solution that ensures complete and secure data protection across up to six hypervisor environments from a unified, touch-friendly, web-based management console. Acronis Backup 12.5 easily and reliably backs up the entire virtual infrastructure, even in multiple hypervisor environments, and protects the newest systems like VMware vSphere 6.5 and Windows Server 2016, with Hyper-V® RCT.

Learn more about our new features such as customizable dashboards, smart alerting, and advanced reporting while trying out Acronis Backup 12.5 . [Download now](#) and be one of the first to experience the best backup solution on the market.