Organizations across the globe are finding disaster recovery increasingly important for a number of reasons. With the two traditional approaches to disaster recovery—workload mirroring and removable-media backups, however, they must choose between spending eighty percent of their disaster recovery budgets on only twenty percent of their server workloads (with cost-prohibitive mirroring), or using inexpensive removable-media backups with much poorer performance.

This white paper explains how virtualization technology can solve the cost versus time dilemma traditional data recovery solutions pose, enabling organizations to quickly and cost effectively recover all server workloads.
<table>
<thead>
<tr>
<th>Table of Contents</th>
<th>page</th>
</tr>
</thead>
<tbody>
<tr>
<td>How to Measure the Value of Disaster Recovery Solutions</td>
<td>1</td>
</tr>
<tr>
<td>Assessing Your Risk through Regular Testing</td>
<td>3</td>
</tr>
<tr>
<td>Changing the Game through Virtualization</td>
<td>4</td>
</tr>
</tbody>
</table>
How to Measure the Value of Disaster Recovery Solutions

The global economy, increased competition requiring just-in-time processes, reduced IT budgets, explosive data growth and new regulatory requirements have all increased disaster recovery’s importance. As a result, organizations are now under pressure to re-evaluate and update their disaster recovery plans.

Looking across the disaster recovery landscape today, we see hundreds of solutions. You should use the following criteria to measure the value of these solutions: cost, performance and risk.

Measuring Total Cost of Ownership

Cost is typically the most important concern for organizations evaluating disaster recovery solutions, particularly during these tough economic times. Ideally, disasters never arise, so IT can find it difficult to secure budget for what should be a system it is unlikely to use. On the other hand, any production server in the data center has some level of business value and is therefore a server worth protecting. With this in mind, organizations must allocate budget appropriately, balancing protection costs against the business importance of data center components.

The significant differences between the two major approaches to server protection further complicate matters. The first approach involves infrastructure mirroring: By mirroring the entire server environment, you can achieve the greatest degree of protection. In the second approach, you simply back up the data within the data center.
Mirroring offers a fully redundant infrastructure, which provides the ability to meet near zero recovery time objectives (RTO, or the total time to recover a service after an outage) and recovery point objectives (RPO, or the tolerance for data loss) performance metrics.

The problem with this approach is total cost of ownership (TCO). Duplicating server workloads doubles the initial cost of every server and also adds to the costs of infrastructure components and bandwidth and implementation and maintenance.

Although you can often justify the expense of duplicating business-critical server workloads such as customer-facing applications (web servers and online order processing, for example), it is harder to find sufficient funds to similarly protect workloads deemed less critical, such as email servers, internal web servers or batch reporting applications.

In comparison, backup solutions leverage everything from inexpensive tapes to increasingly economical disks. As a whole, these solutions tend to be very cost effective. The downside to this data-focused approach is its recovery performance.

The RTO performance of backup solutions tends to be quite poor. It can be time consuming and complex to take backup data from a tape or disk and rebuild it into a usable workload. Think of how long it takes to reinstall and update a server operating system, install and update applications and middleware, and reconfigure all the networking connections, before finally restoring the data. Now what if it’s not just one server, but dozens?

With only these two approaches, your organization must choose expensive, redundant infrastructure or cheap but slow data backup or, typically, some combination of both. Statistics show that organizations end up using eighty percent of their budgets on high-performance protection for only twenty percent of their servers; the ones that absolutely need uninterrupted performance. This leaves the remaining eighty percent of the server workloads under-protected.

**Measuring Performance**

To understand data recovery performance, you should break data recovery into three phases: Backup (or replication), failover and failback.

In most solutions, organizations concentrate on backing everything up. Traditionally focused on the technologies and processes that keep data current, data backup solutions range from simple daily tape backups to sophisticated storage area network (SAN)-based replication.
But a backup copy doesn’t help if you can’t actually use it. You should place equal, if not greater, importance on failover and failback.

As previously discussed, solutions offering the best RTO and RPO performance tend to take complex and expensive redundancy-based approaches. However, organizations that are already facing budget constraints, and have therefore implemented more cost-effective backup solutions, will face lengthy and error-prone failover processes that miss the mark on performance. The processes they use to convert raw data to a useable server workload state are the problem here. Again, cost versus performance is the central challenge.

When planning for disaster recovery, organizations frequently overlook the final phase of the disaster recovery lifecycle: namely failback. With many solutions—even the more cost-effective data backup solutions—they consider only a one-way trip. They have no plan in place to get “back to normal” from the recovery site. Obviously, this can lead to unexpected or unnecessary headaches as they try to return to “business as usual.” Think of failover as putting a temporary spare tire on a car. You can’t keep it on indefinitely; at some point, you have to “fail back” to a regular full-size tire.

Assessing Your Risk through Regular Testing

Most data recovery plans include, at best, an annual test period or event. But, given the speed of business and technology today, in a year, organizations can experience a tremendous amount of change across their data centers and in their business processes. One reason for this inadequate annual testing standard is, again, that most solutions focus on the front end of the disaster recovery lifecycle. The testing process often mirrors the recovery process, and brings with it all the problems and complexities already mentioned with failover. With many disaster recovery solutions, testing can be so cumbersome and disruptive that some organizations don’t do any real testing at all.

Only a thoroughly tested disaster recovery plan can be counted on in a real disaster. All too often, organizations do not adequately test their plans, and thus they do not identify issues until the time comes to execute restore procedures. By then, it is too late.
In addition, organizations typically touch the disaster recovery infrastructure only during these once-a-year (if that) testing periods. If they were able to test more often, in an easier way, their plans would be safer and more reliable, and confidence in them would rise exponentially.

**Changing the Game through Virtualization**

Virtualization enables organizations to change how IT looks at disaster recovery. However, whether it’s because of virtualization technology’s relative youth, its costs or data center regulations and policies, organizations have not adopted virtualization on a large scale for disaster recovery in production environments.

Disaster recovery sites provide relatively safe environments in which to deploy virtualization (as did the test labs in which organizations deployed their first virtual machines [VMs]). And the cost savings you can achieve are compelling.

IT can implement server mirroring with the lowest overall infrastructure investment possible— a virtual infrastructure. You can use one simple, small-footprint virtual server environment to mirror or protect a much larger pool of physical production servers. Virtual machines can provide the flexibility and performance of a “boot in place” workload. Virtualization improves RTO performance by creating a virtual machine backup of the entire workload that you do not have to rebuild from the ground up, as you do with traditional backups.

From a testing standpoint, virtualization enables you to create a snapshot copy of a server workload that you can boot in place and test—not only very easily and quickly, but also with absolutely no impact on production.

With next-generation solutions that leverage virtualization, you can now bridge the gap between mirroring and tape backup when protecting physical servers in the data center. These emerging technology solutions enable you to protect more for less, alleviating the budget concerns of yesterday’s disaster recovery solutions.