Consolidated Disaster Recovery

Traditional disaster recovery solutions cannot keep pace with business requirements for recovery speed and integrity at a reasonable cost. The high cost and complexity of mirroring solutions have forced most organizations to choose which workloads to protect. They can easily justify the expense of protecting the relatively small number of mission-critical server workloads such as customer-facing applications (online order processing, for example), but given budgetary constraints, it is harder to find sufficient funds to protect the more numerous business-critical and business-important workloads such as file servers and internal web servers.

If a server workload is worth running in the first place, it is worth protecting. Recognizing this, IT departments are exploring new disaster recovery alternatives. Server virtualization is one such alternative. Once primarily confined to software development, test and server consolidation scenarios, server virtualization offers significant cost and performance advantages over conventional recovery options.

This white paper explains why a growing number of organizations are now leveraging consolidated recovery solutions to protect the servers that they might otherwise leave under-protected. You will learn how you can use server virtualization with workload portability technologies to implement a disaster recovery plan that is more affordable and flexible than traditional recovery options, while providing rapid restore times and enterprise-level workload protection.
Table of Contents

Disaster Recovery by the Numbers ................................................................. 1
  The 80/20 Problem ............................................................................. 1
  The One-to-One Problem ................................................................. 2

Traditional Disaster Recovery Infrastructures ......................................... 2
  Recovery Metrics ............................................................................. 2

Weighing the Options ............................................................................. 3
  Tape Backup .................................................................................. 3
  Image Capture ................................................................................. 4
  High-End Replication ..................................................................... 4
  Server Clustering .......................................................................... 4
  Demand for Newer Protection Options ............................................ 5

How Virtualization Is Redefining Disaster Recovery and Availability .... 5
  Workload Portability ...................................................................... 5

Protecting Workloads with Consolidated Recovery ................................. 6
  Rapid Recovery ............................................................................. 7
  Ease of Testing .............................................................................. 7
  Consolidated Recovery Extends Data Recovery Capabilities .......... 7

Planning and Implementing a Virtualized Recovery Solution .................. 8
  Planning ....................................................................................... 8
  Implementation ........................................................................... 8

Recovery Hardware Appliances .............................................................. 9

Summing Up ...................................................................................... 9

PlateSpin Disaster Recovery Products .................................................. 10
  PlateSpin Recon .......................................................................... 10
  PlateSpin Protect ......................................................................... 10
  PlateSpin Forge ........................................................................... 10

About NetIQ .................................................................................. 11
Disaster Recovery by the Numbers

In the best of all possible worlds, you would implement high-performance backup and recovery processes for all server workloads regardless of their perceived criticality. Moreover, these recovery processes would be cheap, would have minimal impact on production operations and would be recoverable with a high level of data integrity. In reality, you must always weigh disaster recovery needs against the fiscal need for cost-effectiveness.

Perennially tasked with doing more with less, you must often sacrifice recovery performance because of budgetary constraints. More often than not, economic and technological factors conspire to force you to over-insure a small segment of your server workloads, while underinsuring the lion’s share of your infrastructure.

Disaster Recovery Server Protection Tiers

<table>
<thead>
<tr>
<th>Description</th>
<th>Solution</th>
<th>Protection</th>
<th>Budget</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tier One: Mission-critical</td>
<td>Systems that are vital to running day-to-day business operations</td>
<td>Protected by expensive synchronous or asynchronous data replication to an alternate site in conjunction with an application failover technology like clustering</td>
<td>$$$$$</td>
</tr>
<tr>
<td>applications</td>
<td>without these systems, you can’t conduct business and you are losing revenue</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tier Two: Business-critical</td>
<td>Systems that are critical to ongoing business operations – you can function</td>
<td>Protected by less-expensive replication technology (server-based replication), less bandwidth and no application clustering</td>
<td>$$$$</td>
</tr>
<tr>
<td>applications</td>
<td>without these IT systems for only a short time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tier Three: Business-important</td>
<td>Systems that are important to the business but not critical to running day-</td>
<td>Protected by affordable remote backup or even a third-party remote backup service to an alternate site</td>
<td>$$</td>
</tr>
<tr>
<td>applications</td>
<td>to-day business operations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tier Four: Business-supporting</td>
<td>Systems that support the business but are non-customer-facing and non-</td>
<td>Protected by affordable remote backup, but backups are less frequent</td>
<td>$</td>
</tr>
<tr>
<td>applications</td>
<td>revenue generating</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 1: Disaster recovery budgets over-insure top-tier servers while underinsuring the majority of the server network.

The 80/20 Problem

Organizations typically allocate as much as 80 percent of their disaster recovery budgets to their most mission-critical servers—often as little as 10-20 percent of the total server network. This leaves the remaining 80 percent of servers under protected should the organization experience a server failure or catastrophic site disaster. Although losing any one of these business-critical and business-important servers may not bring the business grinding to a halt, it would impact business and employee productivity and cost time and money. Most organizations would admit that an enterprise-wide disaster recovery plan that adheres to the 80/20 workload protection ratio is deficient. So why do so many organizations spend so much to ensure that only the most critical servers are protected by a disaster recovery solution?
Disaster Recovery Budgets Focus on Tier-1 Servers

Figure 2: Businesses typically spend some 80 percent of their disaster recovery budgets to protect only their tier 1 servers.

The answer is this: Traditional disaster recovery solutions such as server clustering or high-end data replication can be extremely expensive—so much so that organizations can implement them only on a limited basis to protect top-tier servers. In fact they’re so expensive that only large organizations can afford them at all; these solutions are completely cost-prohibitive for most small- and medium-sized businesses.

The One-to-One Problem
Server clustering and mirroring are expensive because they require one-to-one hardware and software redundancy to protect data center assets, resulting in a significantly higher total cost of ownership (TCO). You must maintain exactly the same server configuration at the recovery site as at the production site, with precisely the same operating system versions, application licenses and patch levels installed. Essentially, you must keep a mirror-image of the production data center standing in reserve as a hot standby environment in the event of a downtime event.

Given the high cost of maintaining a mirrored environment and the difficulty of keeping the configuration of the two environments perfectly in sync, most organizations opt to do this only for their top-tier servers, and trust the rest of their server networks to lower-cost alternatives such as tape backups.

Traditional Disaster Recovery Infrastructures
This section provides an overview of the metrics you can use to evaluate the various technology options in the disaster recovery continuum.

Recovery Metrics
The two most common metrics used to evaluate disaster recovery solutions are recovery time objective (RTO) and recovery point objective (RPO), but a third metric, test time objective (TTO), is emerging.
Recovery Time Objective

Recovery time objective (RTO) measures how much downtime an organization can tolerate for a particular computer system or application. It can be anywhere from seconds (including zero) to days, depending on how critical a given workload is. If you know the RTOs, you can determine the types of backup and disaster recovery plans, processes, and technologies that you should implement to protect specific workloads.

Recovery Point Objective

Recovery Point Objective (RPO) is the maximum amount of its most recent data that an organization is prepared to lose in an outage, measured in time (5 minutes, 4 hours, a day and so on). It is generally a time between the last available backup and when a disruption could potentially occur, or put another way, the minimum time between backups. You establish the RPO for a given workload based on your organization’s degree of tolerance for data loss or manual rekeying.

Test Time Objective

Test time objective (TTO) measures the time an organization requires to ensure its disaster recovery plan’s effectiveness through testing. To be confident in their recovery strategies, solutions and methodologies, organizations must thoroughly and regularly test their recovery infrastructures. Routine testing should be relatively easy, quick to implement and non-disruptive to business operations.

Disaster Recovery Metrics

<table>
<thead>
<tr>
<th>RTO</th>
<th>Recovery Time Objective</th>
<th>The Measure of Downtime</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPO</td>
<td>Recovery Point Objective</td>
<td>The Measure of Data Loss</td>
</tr>
<tr>
<td>TTO</td>
<td>Test Time Objective</td>
<td>The Measure of Testing Ease</td>
</tr>
</tbody>
</table>

Figure 3: Businesses evaluate protection and recovery strategies on a per-workload basis according to the objectives in this figure.

Total Cost of Ownership

Although not strictly a recovery metric, TCO is another factor you must weigh when selecting a recovery infrastructure. Some of the questions you need to ask when selecting recovery technologies include:

- How easily can we administer the disaster recovery solution and how many IT personnel do we require to maintain it?
- What specialized IT knowledge do we require to maintain it? How flexible are the replication, recovery and restore processes? Can it handle different RPOs and RTOs for different groups of workloads, or is it a one-size-fits-all solution?
- Does the recovery infrastructure support multiplatform data center environments that may exist today or tomorrow as a result of mergers and acquisitions?

Together, RTO, RPO, TTO and TCO form the basis on which you can develop a cost-effective and efficient workload protection and recovery strategy.

Weighing the Options

To protect server workloads, organizations have a number of different traditional disaster recovery solutions at their disposal. Conventional recovery approaches include tape backup, image capture, high-end replication and server clustering. This section discusses how these solutions stack up in terms of cost, RTO, RPO and TTO.

Tape Backup

Tape backups are the workhorses of most disaster recovery plans. Organizations use magnetic tape to store duplicate copies of hard disk files, not whole server workloads. They typically copy server and desktop-based files to the tapes
using an automated backup utility that updates on a periodic schedule, typically overnight. Many organizations use magnetic tape in combination with magnetic disks and optical disks in a backup management program that automatically moves data from one storage medium to another. They usually store tape archives offsite for recovery purposes; a third-party provider may pick up and store these backup tapes. Because of its low cost per gigabyte, tape backup is the most economically prudent recovery alternative; however, backup utilities and processes can be difficult to administer, as can the logistics of transporting, storing and retrieving tape archives in the event of an outage. It can take hours to restore a system from a backup tape, and days if multiple systems are involved. You must manually rebuild systems (reinstall the operating systems, applications and patch levels) before you can restore the application data.

Image Capture
With image capture, you copy a server workload to an image archive that you then move or replicate to a remote location for disaster recovery. Of course, the further away the image is stored, the longer it may take to physically bring it back to the data center when needed. Many data centers maintain extensive libraries of backup image archives that they can restore to new hardware in the event of a primary workload failure or disaster. Image capture is moderately more expensive than tape backup and can often maintain an adequate RPO, but RTO can be lengthy and error-prone because images are tied to the hardware from which they were captured: You cannot easily recover them to a different server. A common problem is that, when a workload running on an older hardware configuration fails, the data center has no additional platforms of that server make and model to which it can restore the backup image. More flexible image-based solutions enable data centers to capture any image type and restore it to any hardware platform, reducing recovery time and minimizing the aforementioned types of errors and delays.

High-End Replication
You use replication to keep distributed databases synchronized by routinely copying the entire database or subsets of the database to other servers in the network. There are a number of different replication methods. With primary site replication, you maintain the master copy of the data at one site and send read-only copies to the other sites. In a workflow environment, the master copy can move from one site to another. This is called “shared replication” or “transferred ownership replication.” In symmetric replication, also called “update-anywhere” or “peer-to-peer replication,” each site can receive updates, and when they do, all other sites are then updated. Failover replication, or hot backup, maintains an up-to-date copy of the data at a different site for backup. Although replication meets stringent recovery time and point objectives, the technology can be costly, complex and difficult to administer. This data-centric approach also requires one-to-one hardware and application redundancy.

Server Clustering
Server clustering generally refers to multiple servers that are linked together to provide fault tolerance balancing distributes workloads over multiple systems. Clustering achieves near-zero recovery time and point objectives but at a very high cost. Because it can be prohibitively expensive and complicated to implement and maintain, clustering is typically a viable disaster recovery option for only the most mission-critical server environments.

Evaluating Traditional Disaster Recovery Alternatives

<table>
<thead>
<tr>
<th>Solution</th>
<th>RPO</th>
<th>RTO</th>
<th>Cost</th>
<th>Weakness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tape/manual rebuild</td>
<td>24h</td>
<td>Hours</td>
<td>$</td>
<td>• Difficult to administer</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Slow, prone to errors</td>
</tr>
<tr>
<td>Image capture</td>
<td>24h</td>
<td>En Hours ter</td>
<td>$$</td>
<td>• Limited restore and flexibility</td>
</tr>
<tr>
<td>High-end replication</td>
<td>Seconds</td>
<td>Seconds</td>
<td>$$$</td>
<td>• Complicated configuration</td>
</tr>
<tr>
<td></td>
<td>minutes</td>
<td>minutes</td>
<td></td>
<td>• Duplicate hardware</td>
</tr>
<tr>
<td>Server clustering</td>
<td>0</td>
<td>0</td>
<td>$$$$$</td>
<td>• Complicated set-up</td>
</tr>
</tbody>
</table>

Figure 4: This table highlights advantages and weaknesses of the most common disaster recovery approaches.
Demand for Newer Protection Options

Frustrated by the high cost and complexity of some traditional recovery options and the lackluster performance of others, IT organizations are seeking newer protection options that offer a better balance between cost and performance. Many are showing interest in server virtualization as a disaster recovery technology platform. In the next section, you will see how the same features that have made virtualization advantageous for server consolidation and other data center initiatives—namely workload encapsulation and workload portability—are bringing greater flexibility, cost-effectiveness and simplicity to disaster recovery.

How Virtualization Is Redefining Disaster Recovery and Availability

Using virtualization technology, you can configure a single physical server to run multiple virtual machines whereby each instance of the operating system runs its own applications as if it were the only operating system on the server. Virtualization is accomplished by a layer of software called a “hypervisor” that resides between the hardware and the “guest” operating systems. It “abstracts” the guest operating systems from the underlying hardware, making them independent and portable.

The rapid adoption of virtualization technologies has changed the way organizations view the data center. By helping to dissolve the bonds between software and hardware, virtualization has encouraged organizations to see the data center not as a heterogeneous mix of different servers, operating systems, applications and data, but as a set of portable workload units. The ability to profile, move, copy, protect and replicate entire server workloads between physical and virtual hosts is helping many organizations achieve new operational efficiencies and cost savings, and opening up new options for disaster recovery.

Workload Portability

Virtualization alone enables you to move workloads between similar virtual hosts. But using workload portability technologies, you can detach workloads from their native hardware configurations and move a server’s entire software stack to any physical or virtual host, or image archive.

Figure 5: Using workload portability technology, you can migrate workloads across different data center infrastructures.
The increased portability empowers you to move and rebalance server workloads in any direction between physical and virtual hosts—physical-to-virtual, virtual-to-physical, physical-to-physical, in and out of imaging formats, and so on. Workload portability increases data center flexibility, agility and overall efficiency. You can also better address common challenges such as end-of-lease hardware migration, server consolidation, and now, disaster recovery.

Recognizing the technology’s inherent versatility, organizations are beginning to extend server virtualization to new areas of data center operations, including harnessing its benefits to more easily and cost-effectively protect server workloads running in physical or virtual environments. They can copy or replicate physical or virtual server workloads to secondary locations to use as warm standby environments in the event of a primary server outage or site-wide disaster. Virtualization enables you to achieve workload protection by creating a bootable copy of the workload on a virtual recovery platform where you can rapidly bring it back online. As you will see in the next section, virtualization has significant cost and performance advantages over more traditional disaster recovery options such as tape backup, imaging, replication or clustering.

Protecting Workloads with Consolidated Recovery

In a typical workload protection scenario using virtualization, you would replicate multiple workloads remotely over a wide area network (WAN) to a warm standby virtual recovery environment in a different physical site. The replication schedule you choose will depend on the RPO and RTO you need to meet for each workload.

In contrast to data-centric recovery approaches that require system rebuilding, this scenario provides whole workload protection of physical or virtual workloads: consolidated recovery. By replicating the entire workload (data, applications and operating systems), rather than just application data, to a virtual machine environment, everything you need to rapidly recover in the event of an outage is available in a bootable virtual machine on the recovery server.

Consolidated Workload Protection

![Figure 6: Consolidated workload protection allows you to protect multiple physical or virtual workloads using a single virtual recovery server.](image)

Because you can consolidate multiple workloads, whether physical or virtual, onto a single virtualization-equipped recovery server, you do not need to invest in duplicate hardware and software for one-to-one redundancy. Virtualization enables you to use virtual host capacity as a consolidated recovery platform that is more affordable than one-to-one solutions, such as high-end replication or clustering. You can use the cost savings to protect a greater percentage of your workloads, or increase the RPO and RTO of workloads currently protected by tape.

When evaluating workload portability solutions, you should look for live workload replication capabilities or the ability to transfer a workload to an offline virtual machine without taking the production workload offline. Live replication eliminates backup window disruptions and ensures continuous operations.
**Rapid Recovery**

In the event of a primary server outage or site disaster, you can activate the warm standby virtual machine to immediately take over the running of the workload. You can keep the workload running in the virtual recovery environment until you restore the primary server, at which point you can move the workload over to the restored server. You can thus achieve recovery time and point objectives of less than an hour, without high-cost, complex clustering environments.

When planning a virtualized recovery environment and sizing the physical server that will host the recovery environment, you must ensure sufficient compute power and capacity to run the recovery workloads as you normally would for as long as it takes you to restore the production server. If you do not size and provision your physical host appropriately, your workloads may have to run in a degraded state, which could impact business operations.

**Ease of Testing**

To know that your disaster recovery strategy, solution and methodology will meet your needs, you must thoroughly and regularly test it. However, as you saw in the previous section, conventional recovery infrastructures are prohibitively complex and invasive to business operations, making it impractical for you to test them on a regular basis. For many organizations, the first time disaster recovery plans are ever used in production is when an actual disaster happens.

Despite significant investments in disaster recovery, these organizations have no way of knowing for certain how quickly or successfully they can restore their server workloads. This “cross-our-fingers-and-pray-it-works” approach to disaster preparedness isn’t really preparedness at all. As the saying goes, hope is not a strategy.

In addition to being quicker to recover and restore than more costly solutions, virtualized recovery solutions are also much easier to test. Virtualization's inherent testing capabilities make TTO a meaningful recovery metric. The test restore capabilities unique to virtualization allow you to rapidly and easily run test failure scenarios to ensure the integrity of your workload protection plans. Moreover, you can complete routine testing with absolutely no disruption to business operations.

With virtualized recovery, you can run recovery “fire drills” to test recovery plans and assess actual versus target RTO and RPO simply by booting up a replicated copy of a production workload on the virtual recovery server. Because virtualization separates the test workload snapshot from the production network, you can perform testing without affecting the production environment. You can audit recovery plans and processes quickly and easily, and be confident that the recovery solution will work in the event of an actual production failure or disaster.

**Consolidated Recovery Extends Data Recovery Capabilities**

Given the relative affordability for a consolidated recovery solution that leverages virtualization, you can easily justify using virtualization to augment and extend your current disaster recovery capabilities to a broader range of workloads. Virtualized recovery enables organizations of all sizes to protect a greater share of their server infrastructures with minimal capital investments and fewer barriers to implementation.

Different types of workloads require different levels of resiliency and different disaster recovery technologies. Analysts recommend a multi-tier disaster recovery approach that combines different availability and recovery technologies implemented in such a way that they overlap like shingles on a roof. You should opt for a range of recovery capabilities to address applications ranging from low to high criticality. Virtualized recovery enables you to provide more thorough protection for workloads previously deemed too non-critical to warrant the expense of a traditional disaster recovery solution.
Where Consolidated Recovery Fits

<table>
<thead>
<tr>
<th>Solution</th>
<th>Cost</th>
<th>RPO</th>
<th>RTO</th>
<th>TTO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tape backup/manual system rebuild</td>
<td>$</td>
<td>24h</td>
<td>Hours</td>
<td>Days (not practical)</td>
</tr>
<tr>
<td>Traditional Imaging Capture</td>
<td>$$</td>
<td>24h</td>
<td>Hours</td>
<td>Hours (requires additional hardware)</td>
</tr>
<tr>
<td>Flexible imaging</td>
<td>$$$</td>
<td>Hours</td>
<td>Hours</td>
<td>Minutes (no impact on production data)</td>
</tr>
<tr>
<td>Consolidated Recovery using virtualization</td>
<td>$$$</td>
<td>Minutes</td>
<td>Minutes</td>
<td>Minutes (no impact on production data)</td>
</tr>
<tr>
<td>Server clustering</td>
<td>$$$$$</td>
<td>Near zero</td>
<td>Near zero</td>
<td>Near zero (impacts production data, adds risk)</td>
</tr>
</tbody>
</table>

Figure 8: Consolidated recovery bridges the gap between traditional high availability and disaster recovery solutions.

Planning and Implementing a Virtualized Recovery Solution

In this section, you will walk through the steps involved in successfully implementing a virtualized recovery solution for consolidating and protecting production workloads.

Planning

To implement a successful virtualized recovery solution, you need a detailed plan. You must identify the server workloads you wish to protect. You must also profile these workloads by monitoring them over time to ensure that the disaster recovery environment you implement has adequate capacity to support them. The planning phase includes the following steps:

1. **Discover Server Inventory** – Discover and inventory the IT environment, including physical and virtual servers and the data, applications and operating systems installed on them, to identify the workloads you wish to include in your recovery plan.
2. **Monitor Server Use** – Monitor workload information such as CPU, disk, memory and network utilization over a period of time. The information you collect will provide invaluable workload profiling and capacity planning data that you can use as the basis for a recovery plan.
3. **Build the Disaster Recovery Plan** – Create recovery plans to determine the appropriate virtual recovery site capacity. Build enough headroom into your target virtualized recovery environment to ensure sufficient capacity for consolidated workloads in the event of a disaster, and for future expected growth.
4. **Configure the Virtual Recovery Environment** – Match physical production servers with virtual recovery machines and configure your virtual recovery environment.

Implementation

Once the recovery plan has been developed, you will need to perform an initial full replication of source workloads into the virtual recovery environment: perform a live physical-to-virtual migration to stream the entire workload over the network into the virtual machine warm standby environment. After the initial full replication, you will schedule incremental workload replications to synchronize the production server with the virtual recovery environment. The individual RPO you defined for each protected workload will determine the interval between scheduled synchronizations. On each incremental synchronization, the system will copy to the virtual restore system only data that have changed since the previous transfer, not the whole workload.

After you set the synchronization schedule and perform the first replication, you can test the integrity of your disaster recovery plan by powering on the virtual recovery machine within an isolated internal network to ensure the environment is intact, and that performance is adequate.
In the event that a failure or disaster occurs, you can transfer operations from the failed production server to the virtual recovery environment. After this transfer, workloads will run as normal on the virtualized recovery server. After the outage, you can restore workloads in two ways. If you repair the original production server failure and the hardware is intact, you can move the workload from the virtual recovery environment back to the original platform by using a virtual-to-physical workload transfer. If you cannot repair the original hardware, you can restore the workload with a virtual-to-physical transfer onto new, dissimilar hardware.

To recap, the steps involved in implementing the virtualized recovery solution are as follows:

1. **Initial System Backup** – Perform an automated full system backup by transferring whole server workloads (data, applications and operating systems) to the target virtual recovery environment.

2. **Ongoing Incremental Backups** – Automatically propagate all source changes at user-defined intervals to the target virtual recovery environment to ensure that your recovery server contains an exact and up-to-date copy of your production environment.

3. **Test Disaster Recovery Readiness** – Perform a disaster recovery “fire drill” to check application integrity and recovery time. Run a test restore on the backup virtual machine to create a snapshot of the virtual disk file associated with the virtual machine.

4. **Failover in the Event of System Outage** – Should your production server fail, you can initiate a system failover in which the virtual recovery machine rapidly starts up: Just reconnect sessions and the virtual recovery environment takes over the production workload.

5. **Rapid System Restore** – Once your production system is repaired, you can easily perform a virtual-to-physical workload transfer to restore workloads to their original host server or to a new server. You can move data, applications and operating systems from the virtual recovery server to any physical hardware.

### Recovery Hardware Appliances

A purpose-built, consolidated recovery appliance with pre-packaged hardware, software, storage and virtualization components offers many benefits:

- Simplified and accelerated implementation and setup
- Packaged, balanced and right-sized configuration based on the size and criticality of workloads
- Simple, integrated management of the recovery environment as a single entity
- Lower total costs of acquisition and ownership
- Fewer barriers to entry, particularly for small and medium-sized businesses or within departments of larger enterprises

A plug-in-and-protect recovery appliance model offers a dramatically simplified approach to disaster recovery, especially when compared with conventional disaster recovery infrastructures such as replication and clustering. Purpose-built for protecting server-based workloads, a pre-configured and right-sized recovery hardware appliance can reduce or alleviate many of the challenges associated with planning, implementing and maintaining separate software and recovery environments. Even if your organization hasn't invested heavily in virtualization, you can still benefit from an affordable, easy-to-implement virtualized recovery appliance to protect more of your servers.

### Summing Up

Given the compelling cost and performance benefits (affordable consolidated workload protection, rapid recovery capabilities, hardware-independent restore options and ease of testing), organizations are increasingly harnessing the benefits of virtualization to protect a broad spectrum of workloads that have previously gone underinsured.
PlateSpin Disaster Recovery Products

The PlateSpin® product family offers a range of options that can protect entire physical and virtual workloads and provide rapid recovery in the event of downtime or a site disaster.

PlateSpin Recon
PlateSpin Recon profiles all workloads in the data center, collecting inventory and usage data over a standard business cycle to properly identify workloads for protection and select the best recovery option. PlateSpin Recon creates recovery scenarios that match production workloads with recovery resources to ensure a proper fit. Visit www.netiq.com/recon.

PlateSpin Protect
PlateSpin Protect leverages the VMware infrastructure you already own for high-performance protection of both physical and virtual server workloads. Replica workloads created as virtual machines offer extremely fast recovery times, and incremental replication provides multiple restore points. Workloads can be easily restored back to any physical server or virtual host. Visit www.netiq.com/protect.

PlateSpin Forge
PlateSpin Forge® is an all-in-one disaster recovery hardware appliance that delivers high-performance protection of up to 25 physical and virtual server workloads. In the event of a production server outage or disaster, workloads can be rapidly powered on inside the self-contained recovery environment and continue to run normally until the production environment is restored. Visit www.netiq.com/forge.
About NetIQ

NetIQ is a global, IT enterprise software company with relentless focus on customer success. Customers and partners choose NetIQ to cost-effectively tackle information protection challenges and manage the complexity of dynamic, highly-distributed business applications.

Our portfolio includes scalable, automated solutions for Identity, Security and Governance, and IT Operations Management that help organizations securely deliver, measure, and manage computing services across physical, virtual, and cloud computing environments. These solutions and our practical, customer-focused approach to solving persistent IT challenges ensure organizations are able to reduce cost, complexity and risk.

To learn more about our industry-acclaimed software solutions, visit www.netiq.com.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

Copyright © 2015 NetIQ Corporation and its affiliates. All Rights Reserved.

ActiveAudit, ActiveView, Aegis, AppManager, Change Administrator, Change Guardian, Compliance Suite, the cube logo design, Directory and Resource Administrator, Directory Security Administrator, Domain Migration Administrator, Exchange Administrator, File Security Administrator, Group Policy Administrator, Group Policy Guardian, Group Policy Suite, IntelliPolicy, Knowledge Scripts, NetConnect, NetIQ, the NetIQ logo, PSAudit, PSDetect, PSPasswordManager, PSSecure, Secure Configuration Manager, Security Administration Suite, Security Manager, Server Consolidator, VigilEnt, and Vivinet are trademarks or registered trademarks of NetIQ Corporation or its subsidiaries in the USA. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies.

Worldwide Headquarters
515 Post Oak Blvd., Suite 1200
Houston, Texas 77027 USA
Worldwide: +1.713.548.1700
U.S. / Canada Toll Free: 888.323.6768
info@netiq.com
www.netiq.com

www.netiq.com/communities

For a complete list of our offices
In North America, Europe, the Middle East
Africa, Asia-Pacific and Latin America,
please visit www.netiq.com/contacts.

562-001018-001  WJ  03/15