



**Your company relies on its databases.
How are you protecting them?**

Protecting Microsoft SQL Server™



2 Hudson Place – suite 700
Hoboken, NJ 07030

800-674-9495
www.nsisoftware.com

Powered by  **Double-Take**

Executive Summary

Database management systems (DBMS) are the hidden engines behind some of your most critical information applications. The types of critical business applications that depend on DBMS include:

- Enterprise Resource Management (ERP)
- Customer Relationship Management (CRM)
- Accounting
- Sales force automation
- Order tracking
- Inventory management
- Technical support and customer service help desks

In most cases, all of the data for these business systems is stored in a DBMS. This means that if the DBMS is damaged, not only is the application unavailable, but all the current and historical data is at risk. One of the most common DBMS for Microsoft® Windows® servers is Microsoft SQL Server™ (MS-SQL). Depending on your environment, your Microsoft SQL Server may be your most critical application.

Like most database management systems, MS-SQL stores all of the data in a handful of database containers, or files. If one of these containers is damaged or corrupted, all of the data it contains is lost. ***The end result - a serious failure of one system could close the doors of your business for days, even permanently.***

This white paper discusses data protection strategies for Microsoft SQL Server, and answers the following questions:

- What does it really mean to protect a database?
- What are the alternatives?
- How do I compare the costs and advantages of different solutions?
- Why should you consider NSI® Software?

What does it really mean to protect a DBMS?

There are two phases to a DBMS protection strategy:

1. Data Protection - Ensure you have a second copy of the data
2. Data Availability - Prepare the redundant data and application to be brought on-line in case the primary becomes unavailable

Each phase may be easy or difficult, depending on your existing technology, procedures, and objectives.

For example, most MS-SQL administrators already back-up their databases, typically to tape. For some, it may appear that this satisfies step 1, however with further discussion it is likely that this will not meet their particular business needs. At some point, typically during night time off-hours, database administrators back up their DBMS, most likely to tape, creating a second copy of the database. But, how good is that data at noon the next day? Any data that has been entered into the database since the backup probably does not exist anywhere else and would have to be manually recreated.

To determine if a particular data protection strategy is appropriate you first need to understand the key data recovery metrics and then define your recovery objectives using these metrics.

The first key metric is Recovery Point Objective (RPO). RPO defines how much data will be lost in the recovery procedure. If a single disk drive in a RAID 5 array fails, you would lose no data - this is an RPO of zero. If the entire disk array fails and you have to restore from tape, you will lose all the data added to the database since the backup. This is an RPO of 12-24 hours, assuming the last backup is usable.

The second critical metric is Recovery Time Objective (RTO). RTO measures how long the entire recovery process takes. If a virus corrupts a database, and you simply need to restore it from tape, you may be able to accomplish this in an hour or two, often times longer depending on the size of the database. This is an RTO of around two hours. If an entire server must be replaced, the RTO may be greater than 24 hours, depending on how long it takes to replace the drive, retrieve the tapes, and restore the data. Once you have quantified your recovery objectives, you are likely to discover that traditional tape backup will not be good enough to achieve your RTO and RPO goals for your critical DBMS applications. Especially when you consider that you need to protect against multiple types of failure scenarios, including individual server or device failure and site-wide disaster.

- **Individual server failure scenario.** Even if the repair is simple, the RTO from tapes, especially if they are stored off-site, may be unacceptably long. In addition, the RPO in this scenario is likely to be very poor as you will lose all data since the backup was taken. If your business cannot tolerate the down time or the data loss, then you need a High Availability (HA) solution. HA solutions are designed to recover from a single server or device failure with very low RTO and RPO and ensure data and applications remain seamlessly available.

According to Forrester Research, most large, online businesses average one to five hours of downtime every month, and lose \$8,000 or more per hour.

- **Site-wide disaster scenario.** In this scenario, the entire datacenter is unavailable. This disaster may come in the form of a natural disaster, power outage, industrial accident, or even peripheral emergencies that may not directly affect your facility, but prevent access to it. Disaster Recovery (DR) solutions should provide a very low RPO, meaning little to no loss of data, and often but not always a low RTO, allowing your business to be back online ASAP. These solutions generally involve copying data offsite, and may provide for starting and running of the application at the remote location.

What are the alternatives when low RPO and RTO are required?

When the RPO and RTO must be kept low, hardware-based synchronous replication is a potential data protection alternative. Synchronous replication is usually accomplished by connecting two SAN disk subsystems via fiber optic cable. Synchronous replication or mirroring can provide zero data loss (RPO), and with proper configuration, may provide an RTO measured in minutes. However, these hardware-based solutions are very expensive to purchase and operate, and have distance limitations of about 10 miles. The distance limitation means these solutions are typically inadequate for Disaster Recovery since both locations that are within 10 miles of each other could be impacted by the same crisis. Most business data does not require this level of protection; absolutely zero data loss. While some may, generally this level of RPO can not be cost-justified.

Replication for the Masses

NSI Software Double-Take[®] provides patented asynchronous replication technology that fills the vast middle ground between tape backup and synchronous mirroring solutions. Double-Take solutions can be configured to provide RTO and RPO measured in minutes, and often in seconds, with low purchase and operational costs. Without a distance limitation, Double-Take is equally capable of providing HA and DR solutions. In figure 1, you can see that Double-Take provides dramatically improved protection with only a moderate additional cost compared to tape solutions.

A Yankee Group and Sunbelt Software survey of 362 IT executives in March 2004 found **42 percent of respondents had been unable to recover data from tape in the last year as a result of tape unreliability.**

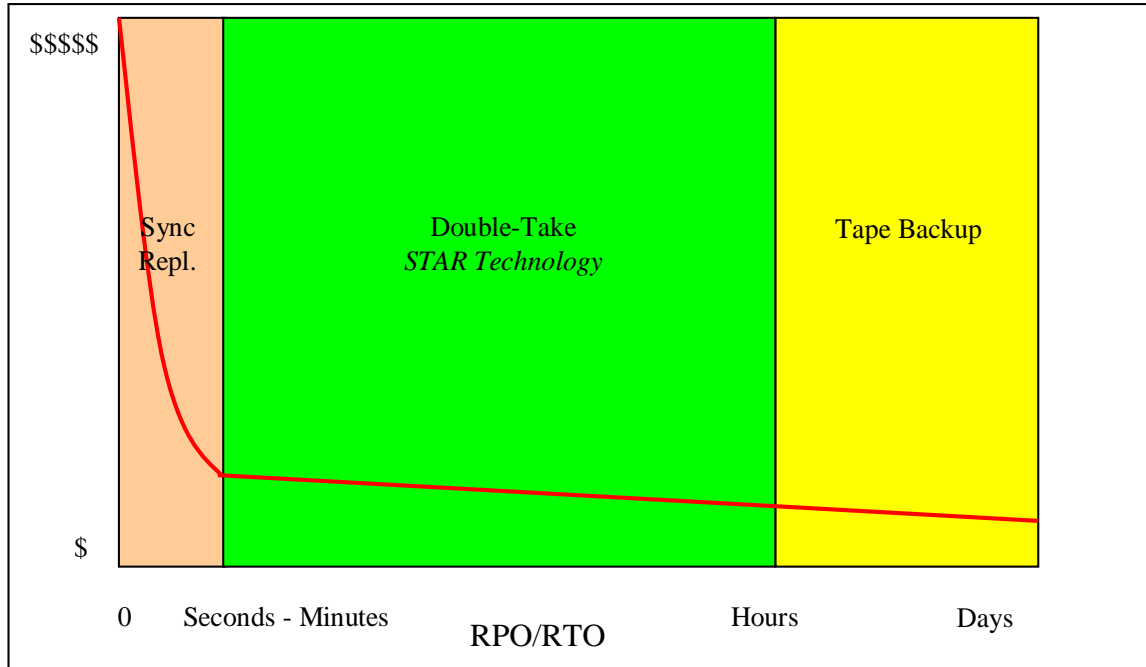


Figure 1 – RPO/RTO Relative to Cost

What about MS-SQL's built-in replication capabilities?

MS-SQL's built-in replication feature is designed to publish periodically updated, read-only copies of selected data. It is not designed to provide data protection or application availability to the entire database.

The built-in recovery capability provided by MS-SQL is called 'log shipping'. This technique assumes that a recent copy of the database exists, possibly on tape, and can be restored on another server to create the baseline copy of the database. Once the baseline is established, Microsoft SQL Server periodically sends a log of recent transactions. These transactions can be applied to the copy of the database to bring it up-to-date. This updated copy of the database can then be used to replace the failed production system if needed.

Typical challenges with log shipping include:

- Data integrity cannot be maintained across multiple databases
- Potentially significant processing overhead during production hours
- Logs cannot be shipped more often than once per minute, and are typically shipped less often - increasing the amount of lost data after an outage (RPO)
- Un-logged transactions are not included
- Advanced administrative skill is required
- No automatic failover mechanism
- Tracks data changes only, not schema, security, or other DB changes

In contrast, Double-Take automatically includes all changes to the data, including:

- Schema updates
- Security configuration
- Bulk transactions
- Real-time replication to the replica
- Automatic, transparent failover
- *Plus, no changes to the MS-SQL configuration are required to get complete protection using Double-Take*

How NSI Software technologies deliver MS-SQL HA and DR solutions

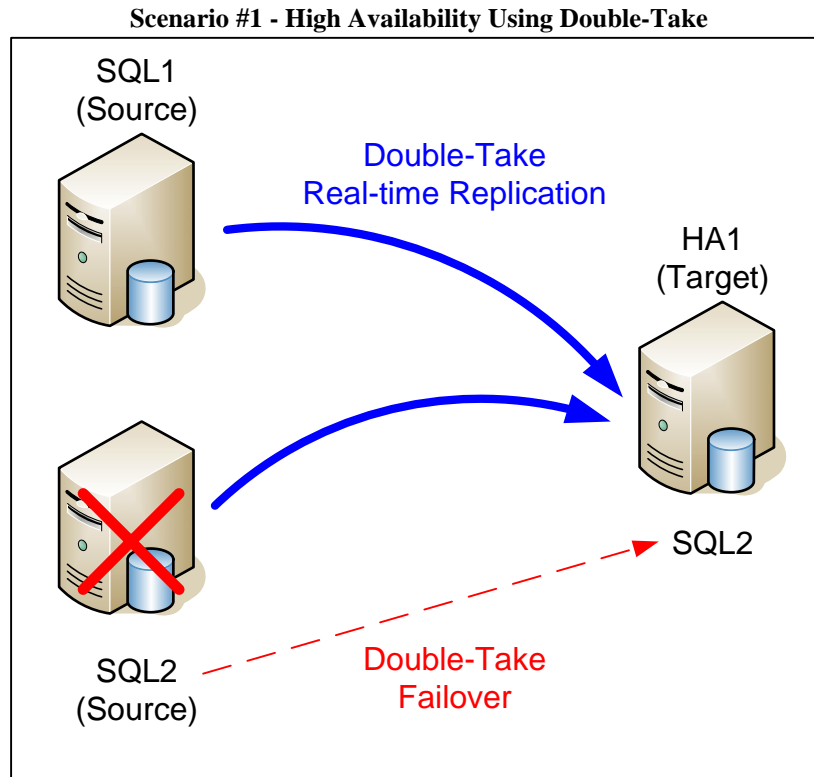
Complete protection of MS-SQL Server requires a High Availability (HA) solution and a Disaster Recovery (DR) solution. Each solution must have a defined RTO and RPO, and the solution architect must balance the cost of achieving those values against the cost of downtime and lost data. This section examines several scenarios, and identifies the type of NSI solution for each.

Scenario 1 - High Availability using Double-Take

Double-Take is designed for "many-to-one" replication between Windows server platforms across an IP network. A single target server on the same LAN can provide High Availability for one large production server, or for several smaller production servers. With the continuous replication and built-in failover capabilities within Double-Take, it is possible for the target server to stand in for a failed server(s) in a matter of seconds. The target server will appear on the network with the same identity, same MS-SQL configuration, and with data that is within a few seconds of the failed server. This solution provides users with near-instant access to their data often without ever knowing there was a failure.

"A rolling blackout or earthquake could cost us \$145,000 a day in lost productivity if our people do not have access to a mission-critical application on our server. With NSI Software's Double-Take, even disaster can't keep us down for more than 5 minutes; access is uninterrupted."

**Robb Good, Vice President,
Director of Information
Systems, Sundt
Construction, Inc.**

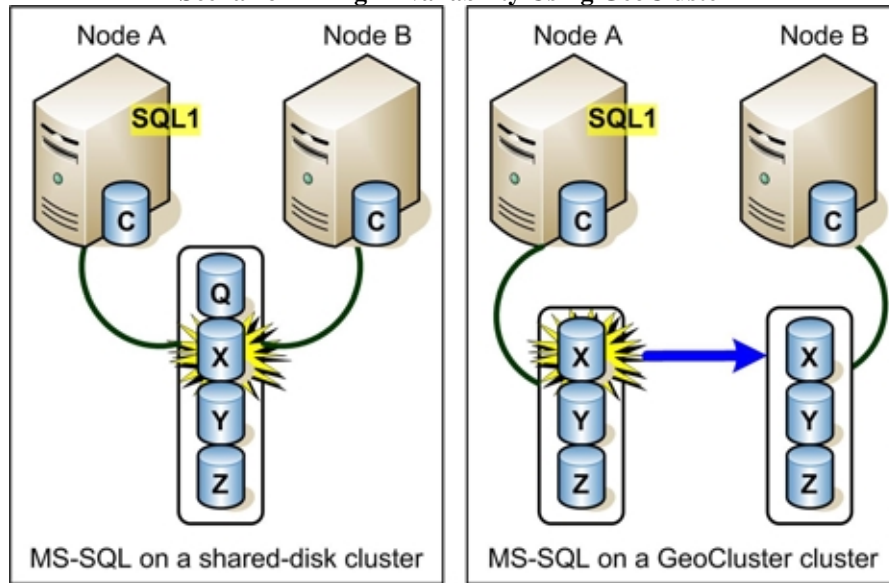


Scenario 2 - High Availability using GeoCluster®

Traditional hardware clusters use multiple nodes and a shared disk subsystem to provide excellent application availability, but they still have a single point of failure in the disk storage sub-system. Should this disk subsystem fail, the entire cluster is rendered unavailable. NSI Software created GeoCluster® to enable a Microsoft Cluster Server cluster to have separate redundant storage - providing both application availability and data protection. GeoCluster utilizes the patented Double-Take replication engine to ensure each node maintains an exact copy of the active data. Each node in the cluster can now have its own exact copy of the data on its own storage device. Should the active node fail, MSCS will automatically fail over the failed server to one of the other cluster nodes that has maintained an exact replica of the failed disks data. GeoCluster also provides the ability to configure Microsoft clusters using any non-similar storage devices. One node could have internal disk while another could be connected to a disk array. This reduces overall costs of deploying Microsoft clusters and simplifies management.

"With GeoCluster, we are saving thousands over the alternate solutions."
Steve Wagner,
Manager, Abbey Press
Information Systems
and Services

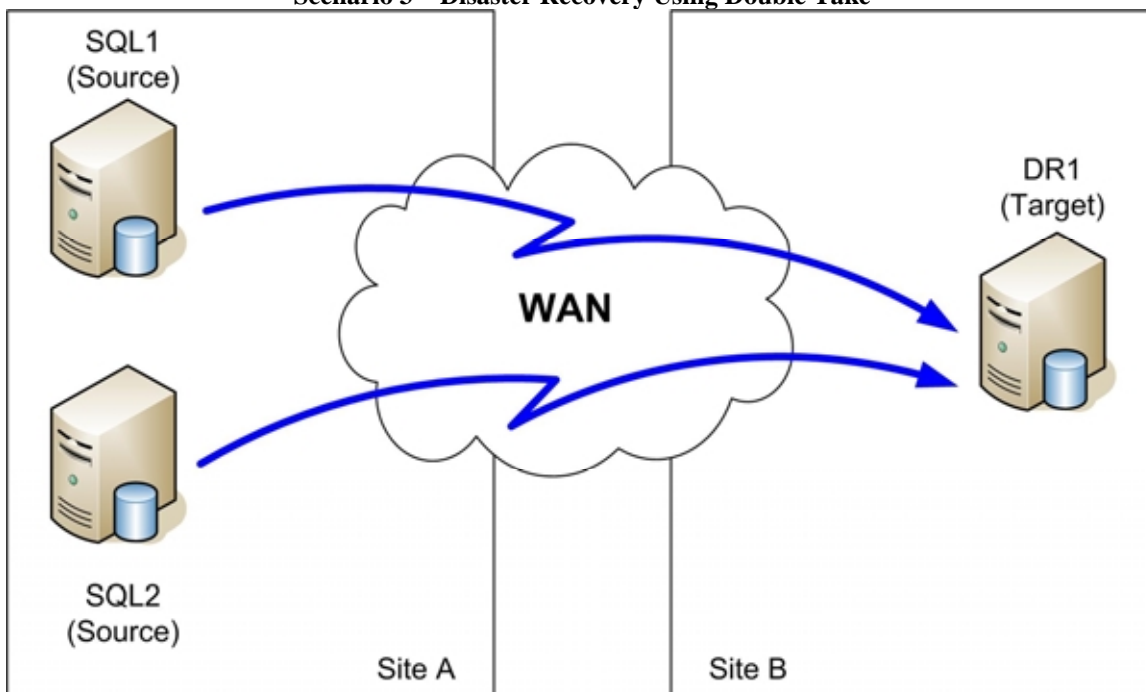
Scenario 2 – High Availability Using GeoCluster



Scenario 3 - Disaster Recovery using Double-Take

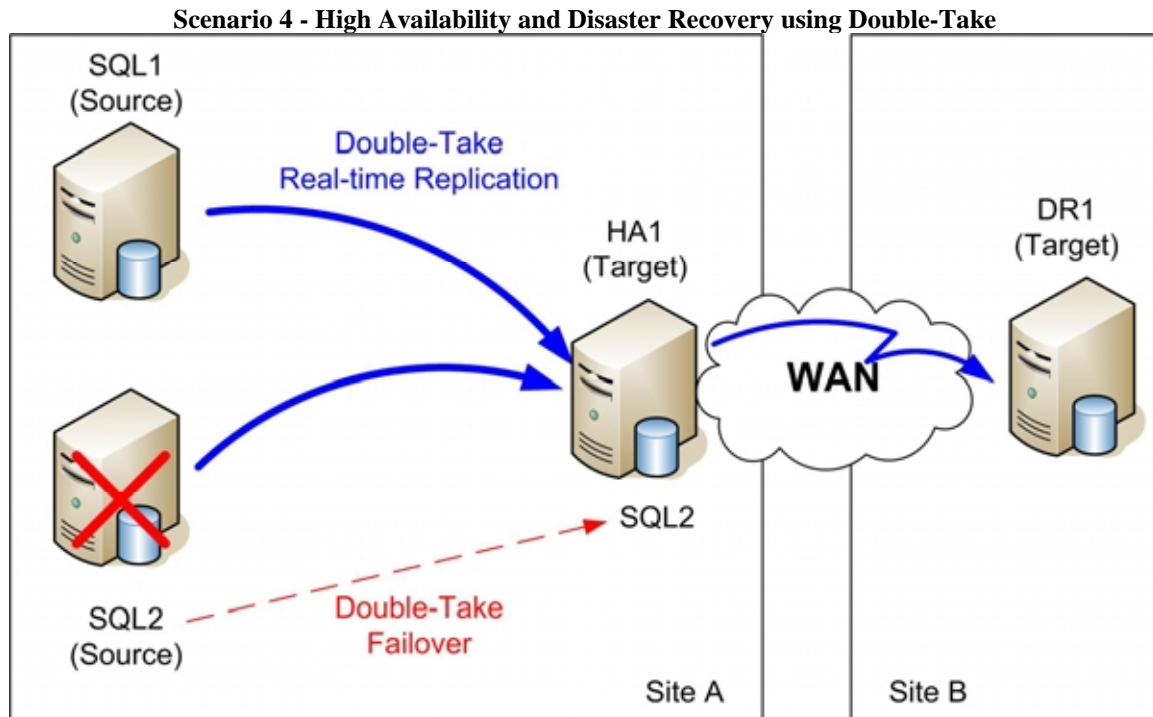
The most fundamental feature of a Disaster Recovery solution is that the target servers are placed at a remote location to where production data is continuously copied. DR solutions based on Double-Take can protect against an entire datacenter or regional failure by allowing data to be copied many miles away. By using Double-Take with existing facilities and WAN links, you can implement and operate a high quality DR solution at a very low cost. This DR solution has no distance limitations, so the recovery center can be placed as far away as necessary to avoid common risks.

Scenario 3 – Disaster Recovery Using Double Take



Scenario 4 - High Availability and Disaster Recovery using Double-Take

Double-Take supports combinations of "many-to-one" and chained configurations to deliver a combined HA and DR solution. The HA server at Site A provides low RPO and RTO protection against an individual server failure, while the DR solution provides remote replication to one or more servers at a remote facility that is accessible via the WAN, and provides protection against an entire site failure.



Scenario 5 - High Availability and Disaster Recovery using GeoCluster and Double-Take

NSI Double-Take provides the same level of disaster recovery protection for Microsoft clusters as it does for standalone servers. Although a cluster may be protected from an individual server or disk failure, it is not protected from a site failure and should still be considered for remote replication. Double-Take is designed to work within Microsoft cluster environments to ensure appropriate data from active resources is replicated to an offsite DR location, regardless of which cluster node controls the resource. With GeoCluster ensuring that your Microsoft cluster is well protected from a disk or server failure, Double-Take ensures it is protected from a complete cluster or site failure.

How Double-Take can meet other data protection, availability, migration, and distribution needs

In addition to protecting your MS-SQL data, Double-Take can provide powerful solutions for a number of data protection, data availability, data migration, and data distribution challenges.

Scenario 6 - NAS to SAN storage migration. As more environments move from direct attached storage to NAS or SAN, the question of how the actual migration will occur becomes more frequent. Using the same techniques outlined above for data protection, one can migrate from local storage to a NAS, a server utilizing a SAN, or even a NAS-gateway to the SAN. In all cases, the fundamental requirement is that the data is moved from one Windows platform (with local storage) to another Windows platform (with more manageable storage), like that of a Windows-Powered NAS (or Storage Server). A huge advantage of using Double-Take for migrations is that the data is continuously updated on the new server/storage, allowing users to be cut over at any time. It is not necessary to stop all user access in order to move the data. Plus, since the replica can be write-enabled, users don't have to be moved all at once.

Scenario 7 - Branch office server to Centralized Data Center. Even in the enterprises where protecting the corporate data has become a standard, branch offices tend to still be isolated to tape solutions. This forces non-VT personnel to be responsible for tape rotations and cleanings. The result is higher manpower costs and lower restore reliability. By efficiently replicating the byte-level changes within the data at the branch offices using Double-Take, one can bring the branches' data back to a centralized data center. This provides disaster recovery for the branches, and allows backups to be managed at the centralized facility by I/T personnel using more advanced tape technologies.

Scenario 8 - Small office Server-to-Server Protection. Large enterprises may have multiple data centers and a myriad of server technologies, but the typical small office relies heavily on few servers, often with limited I/T resources or personnel. When the primary server fails, the office productivity can grind to a halt. Double-Take provides a simple and cost-effective way to "fail over" to a second machine, either in the same office or perhaps even at an employee's home. The result is rapid availability of the data - and the small office continues doing business.

"Double-Take was the optimum solution that integrated smoothly with our core application. In fact, Double-Take's flexibility made it the only option."

*Christina Surmenean,
Senior Vice President and
CIO for CNA Trust*

Scenario 9 - Consolidate Backup Operations. Today's corporations are increasing their business day, as geographic and national boundaries no longer limit effective commerce. This results in an ever shrinking backup window. However, the redundant copies of files on Double-Take target servers can be backed up at any time, even when the original copy of data is in use. Without expensive and application-specific backup agents, the second copy of the data can be put to tape using existing tape technology attached to the redundant server. And perhaps even better, the backup can be done at local disk/tape speeds, instead of a media server backing up multiple application servers. This increases the backup window and ensures there are not missed files due to them being open.

Scenario 10 - Data Distribution. Many replication needs are not based around data protection or availability. Like the migration solutions discussed above, some business goals simply need to get the data to an alternate location. Double-Take can provide a corporation with a master-content server and then ensure that all regional locations and branch offices receive the replicated files - regardless of whether it is a custom application or simply the Human Resources directory for vacation forms and business card requests

Why NSI Software?

NSI Software has been providing software that improves the performance and availability of networks since 1991, and has been protecting Microsoft SQL Server databases on Windows servers since 1996. We have deployed production solutions on MS-SQL 6.5, 7.0, and 2000, for healthcare, legal, financial, energy, government, and other businesses. We have been in this business for a long time, and we make sure we do it better than anyone else. With over 25,000 licenses shipped, we are by far the largest supplier of Windows host-based replication software in the industry.

At NSI Software data protection is our only business, and we make it our business to do it better than anyone else. "Business Continuity through Replication" is the single focus of every person in our company. That focus, and the quality of our products, has helped NSI forge relationships with IBM®, Dell®, SunGard®, Microsoft® and probably your preferred reseller-integrator.

Some of the leading server hardware vendors, including Dell, HP and IBM, endorse Double-Take for their own customers. In addition, Double-Take is the de-facto cross-platform replication standard for the Windows powered NAS market.

Please visit www.NSIsoftware.com for more information on Double-Take, including information on how to migrate your existing servers, how to replicate data for business continuity, and how to improve and centralize backups.



For more information on NSI Software's products and services, please contact NSI.

NSI Software, Inc. - Corporate Office
 Two Hudson Plaza, Suite 700
 Hoboken, NJ 07030
 800-775-4674 or 201-656-2121
 Fax: 201-656-2727

NSI Software, Inc. – Inside Sales
 8470 Allison Pointe Blvd. Suite 300
 Indianapolis, IN 46250
 800-674-9495
 Fax: 317-598-0187



Or visit us on the web at WWW.NSISOFTWARE.COM

© 2004 NSI Software, Inc. All rights reserved.

Double-Take®, NSI® and GeoCluster® are registered trademarks of NSI Software, Inc., Balance™ is a trademark of NSI Software, Inc. and all are used with permission of the trademark owner. All other trademarks are properties of their respective companies.

Microsoft, Windows Powered, Windows, Exchange, and Microsoft SQL Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Although we try to provide quality information, NSI makes no claims, promises or guarantees about the accuracy, completeness, or adequacy of the information contained in this document. Companies, names and data used in examples herein are hypothetical and/or fictitious unless otherwise stated.