STORAGE

A practical guide to iSCSI storage

It's safe, reliable and quick enough for most critical apps—find out how your company can take advantage of iSCSI storage.

Vendor resources

iSCSI security

iSCSI case studies

iSCSI vs. FC

iSCSI and VMware

iSCSI storage
is here
to stay

By Rich Castagna

WHEN iSCSI FIRST ARRIVED five years ago, there were plenty of people who hopped on the bandwagon—and even more who rolled up their sleeves to give it a good push. This new way of doing block storage using ordinary Ethernet seemed almost too good to be true. What was too good to be true was all the hype surrounding iSCSI—and, I have to admit, I was one of those "hipsters."

Everything looks different when you acquire the perspective that the distance of a few years affords, along with a little context called reality. So while the predictions that iSCSI storage was so simple, so inexpensive and so easy to use that it would steamroll Fibre Channel into the annals of history were, let's say, a little too exuberant, it's clear now that iSCSI storage is here to stay.

Of course there were naysayers back at iSCSI's dawn. They said it's too slow, it's not reliable and what about security? All of those cavils were true to some extent, but the iSCSI systems of today have moved well beyond most of those original criticisms.

With 1TB disk drives—and larger ones that are here already—and some tinkering under the hood, along with speedier Ethernet connections, iSCSI storage systems can stand up to most of what any small, medium or big business can throw at them. As such, they've found a niche in many of those companies, as primary storage, secondary tiers and effective disk-based backup systems.

In some of *Storage* magazine's recent surveys, there is compelling

> This new way of doing block storage using ordinary Ethernet seemed almost too good to be true.

evidence that iSCSI storage has gained more than a mere foothold. For example, in our Spring 2008 Purchasing Intentions survey, 40% of respondents said they had already deployed or planned to deploy iSCSI storage this year. And the number of those companies planning to use iSCSI for mission-critical applications has grown dramatically, with 42% saying that iSCSI will suit their key apps just fine—a full 10-point jump in less than a year.

This eZine is intended for fence-sitters who may still have lingering doubts about iSCSI, for those who are already sold and are looking for new ways to deploy iSCSI systems, and for those who are weighing the relative merits of Fibre Channel and iSCSI storage. iSCSI might not be the proverbial elephant in the room just yet, but it's too compelling to ignore. ⊙

Rich Castagna is Editorial Director of the Storage Media Group.

iSCSI and VMware

VMware's support for iSCSI has led to a new legion of users who are running virtualized servers quickly and cheaply on iSCSI SANs.

By Christine Cignoli

HE MARRIAGE OF VIRTUALIZED SERVERS and iSCSI SANs is turning out to be a happy one for many users. Since VMware announced support for iSCSI SANs in June 2006, virtualization users have embraced iSCSI's lower cost and reduced complexity.

Two years later, the honeymoon still isn't over. Pat O'Day, chief technology officer at BlueLock, an Indianapolis-based provider of infrastructure as a service, says his young company has used only VMware and LeftHand Networks' iSCSI SANs in its two-year existence. "We were fully prepared that at some point we would have to investigate going into Fibre Channel," he says. "I still have it way out on the radar. But we're up to 50TB or 60TB now."

Cost and flexibility drove BlueLock's selection of iSCSI. O'Day calls iSCSI "a very loose technology. Fibre Channel is so physically dependent on the infrastructure." iSCSI makes it easy to boot servers from BlueLock's main facility to its Salt Lake City data center, he says.

iSCSI's lower cost was worth the slight performance difference. "Fibre Channel drives certainly are a little faster," says O'Day. "But they're not 300% faster."

Matt Simmons, network infrastructure manager at Golf Savings Bank in Mountlake Terrace, WA, also cites cost as his reason for choosing iSCSI over Fibre Channel. The bank has been using VMware Infrastructure 3 in conjunction with EqualLogic iSCSI SANs for about two years. "You get so much more bang for your buck," he says.

Golf Savings did run into a performance bottleneck as the bank grew. "We had to step up to some beefier backplane switches to get the most performance out of them because we really hit them pretty hard," says Simmons.

iSCSI vendors EqualLogic (now part of Dell) and LeftHand Networks (which has been acquired by Hewlett-Packard Co.) have seen an influx

of customers since VMware's June 2006 decision. EqualLogic's product marketing manager, Timothy Sherbak, says, "Definitely, enterprise customers have increased by virtue of virtualization."

Ben Bolles, director of product management at LeftHand Networks, says their adoption rates also went up after VMware's endorsement. "There's a certain majority of the customers that aren't going to deploy a particular technology until that vendor gets behind it," he says.

iSCSI is also making its way into virtualized server environments as a complement to FC. Bill Montgomery, manager of information systems at Lulu.com, says that his company uses iSCSI for everything but backend storage and e-commerce databases, which are handled by Fibre Channel. "For general business computing, iSCSI is going to satisfy the performance requirements of 95% of your applications," he says.

Montgomery also likes iSCSI's simplicity. "Everything about Fibre Channel costs more, and it's not as easy either," he says. "A couple years ago it seemed like [iSCSI] had gotten to the point where it was mature enough technology to be able to rely on it."

Lulu.com encountered some issues with firmware versions between the iSCSI SAN and its HBAs, but "it was nothing that prevented us from implementing something that we wanted to do," notes Montgomery. He adds that the company's iSCSI HBAs, which are used to boot diskless blade servers, are the key to keeping processes simple and flexible.

Greg Schulz, senior analyst and founder of StorageIO Group, a consulting firm in Stillwater, MN, views the two technologies as intertwined. "You could make the claim that virtualization is the key to iSCSI or [that] iSCSI is the key to virtualization," he says. Schulz predicts an upward trend in iSCSI adoption as IP comfort levels shift. There's still baggage, he says, "but barriers are dropping faster."

Golf Savings Bank's Simmons isn't looking back. "I have not heard a compelling reason why I need Fibre Channel," he says, "other than you need to spend more money." ◉

Christine Cignoli is associate editor of the Trends section for *Storage* magazine.

iSCSI vs. FC

Upstart storage protocol iSCSI has come into its own with proven reliability and performance.

By Stephen J. Bigelow

HE LANDSCAPE OF SANs IS CHANGING, and the established boundaries of Fibre Channel vs. iSCSI SANs are blurring rapidly. These days, you can build a Fibre Channel SAN for less than $10,000, but you can also spend $1 million on an iSCSI SAN or run database applications from NAS. There are no absolute rules on what you can and can't do when it comes to Fibre Channel and iSCSI. However, there are pros and cons to each approach that you'll need to consider.

TECHNOLOGICAL DIFFERENCES BETWEEN iSCSI AND FIBRE CHANNEL

All SANs connect servers to shared block storage arrays through a dedicated high-speed network of host bus adapters (HBAs) and switches. The resulting storage network allows servers and storage to communicate, and multiple pathways can be established to ensure storage availability by enhancing redundancy and improving performance. The SAN is also configured to limit the visibility of storage to particular servers or applications.

SANs have traditionally employed the Fibre Channel protocol using the physical implementation and signaling detailed in ANSI standard X3.230-1994 (ISO 14165-1). Fibre Channel uses optical fiber, coaxial copper or twisted pair copper cabling to carry SAN data at speeds of 1Gb/sec, 2Gb/sec, 4Gb/sec and 10Gb/sec. Fibre Channel can operate in point-to-point, switched and loop modes.

However, Fibre Channel has been criticized for its expense and complexity. For example, a specialized HBA card is needed for each server. Each HBA must then connect to a corresponding port on a Fibre Channel switch—creating the SAN "fabric." Well-known HBAs include the Atto Technology Inc. Celerity FC-44ES HBA, the Emulex LPe1150, PCI

Express 4Gb/sec HBAs, the LSI Corp. LSI7404EP-LC HBA and the QLogic Corp. QLA2462 4Gb/sec Fibre Channel HBA. Brocade and Cisco Systems Inc. provide a range of high-performance intelligent SAN switches.

Every combination of HBA and switch port can cost an organization thousands of dollars. Once LUNs are created in storage, they must be zoned and masked to ensure that they are only accessible to the appropriate servers or applications. These processes add complexity and management overhead to Fibre Channel SANs.

The cost and complexity of Fibre Channel kept SAN deployment out of reach for small- to medium-sized businesses (SMBs) until the introduction of Storage over IP SANs based on the iSCSI protocol ratified by the Internet Engineering Task Force in 2003. There is nothing new about the idea of sending storage data over an IP network; the FCIP and iFCP protocols specify the means of sending Fibre Channel data over IP networks. But iSCSI is the first protocol that allows native SCSI commands end-to-end over IP.

iSCSI emphasizes the idea of a "pervasive" Ethernet environment. That is, every organization from the smallest home network to the largest enterprise uses Ethernet LAN technology that is well understood and inexpensive. In actual practice, an iSCSI SAN should employ high-quality network interface cards (NICs) and Ethernet switches in a segregated network. Some organizations try to improve iSCSI performance by deploying Ethernet NICs with TCP/IP offload engine (TOE) features to reduce the CPU demands for iSCSI command processing.

But at the most basic level, an iSCSI SAN can be implemented using existing NICs and switches that are running on the LAN now. Today, most iSCSI SANs operate at 1Gb/sec Ethernet speeds, but some are starting to run at 10 Gigabit Ethernet (GbE) as NICs and switches are upgraded to accommodate 10GbE.

Every combination of HBA and switch port can cost an organization thousands of dollars.

The appeal of iSCSI is easy to understand. Instead of learning, building and managing two networks—an Ethernet LAN for user communication and a Fibre Channel SAN for storage—an organization can leverage its existing Ethernet knowledge for both LAN and SAN. "We believe that having an end-to-end Ethernet IP environment provides a lot of value in terms of skill sets, equipment and commonality in services, capabilities and software tools," says Tony Asaro, formerly the senior analyst with the Enterprise Strategy Group (ESG), now chief strategy officer with Virtual Iron Software.

It's important to know that an iSCSI SAN isn't the same as NAS, even though both use the same IP/Ethernet network. An iSCSI SAN provides block-level access to data (it gives you a disk drive) where NAS provides file-level access to data (it serves up a file). The choice of whether to implement iSCSI or NAS will depend on the apps accessing the storage.

PERFORMANCE DIFFERENCES
Fibre Channel and iSCSI are about equally able to handle storage applications, though experts agree that iSCSI may encounter performance limitations with the most demanding applications. "Most people com-

pare bandwidth with performance, which is not a direct correlation," Asaro says. "It's only in bandwidth-intensive applications where an Ethernet environment might run out of bandwidth and become a [performance] bottleneck." Extremely demanding applications, such as OLTP handling a large number of small transactions, can be adversely affected by the packet overhead in an IP environment. A properly designed iSCSI infrastructure and storage platform should be able to handle any storage application currently handled by a Fibre Channel SAN.

In fact, concerns about iSCSI performance and reliability are largely misplaced. "The highest performing SAN that I ever saw was an iSCSI SAN, not a Fibre Channel SAN," says Stephen Foskett, director of data practice at Contoural Inc. in Mountain View, CA. And users are deploying iSCSI in core applications. ESG research found that 50% of iSCSI early adopters are using iSCSI for mission-critical applications, which is a strong statement of support for iSCSI reliability.

One potential problem with Ethernet performance is the common practice of oversubscription. Most Ethernet servers don't need high performance, so almost all Ethernet switches are oversubscribed. A port may be oversubscribed by as much as 10 to 1. In a high-performance iSCSI SAN, those oversubscribed switches may not be able to handle the load, so you may want to select high-end Ethernet switches for deployment in an iSCSI SAN.

iSCSI performance may also be influenced by the choice of software-based iSCSI initiators or purpose-built iSCSI HBAs, instead of a conventional NIC. Dedicated iSCSI HBAs include Alacritech Inc.'s SES2100 Accelerator card, the Magic 2028-4P 1Gb Copper TCP/IP Accelerated NIC from LeWiz Communications Inc. and the QLogic Corp. QLA4050C iSCSI HBA. Most software-based initiators perform well for general-purpose computing, so they aren't essential now. But the broad introduction of 10GbE may require a shift toward hardware-based initiators. For now, it's important to use the most mature iSCSI initiator software.

Another wrinkle with iSCSI initiators may appear in virtualized environments. Contoural's Foskett points out that the VMware ESX Version 3 initiator has received complaints about its performance in large-scale deployments, because VMware is extremely demanding of CPU and storage. "Once you have a dozen servers sitting on one VMware ESX box, you can really use a lot of storage performance," Foskett says. The suggestion would then be to buy the dedicated iSCSI HBAs.

> **The simplicity of iSCSI in its use of existing Ethernet components makes iSCSI easier and faster to deploy.**

IMPLEMENTATION DIFFERENCES

The simplicity of iSCSI and its use of existing Ethernet components makes iSCSI easier and faster to deploy. ESG research suggests that companies may realize savings of 10% to 30% in iSCSI capital expense and ongoing operational costs compared to Fibre Channel. With recent advances, however, it is actually possible to spend more

money on iSCSI than on Fibre Channel.

Foskett notes that the latest iSCSI storage arrays implement architectures that perform well and scale easily. This is heralding integrated features like thin provisioning, subdisk RAID and automated tiered storage, which may not be readily available in Fibre Channel arrays. iSCSI arrays are also noted for their scalability, making it easy to buy and deploy additional iSCSI arrays over time with little (if any) direct management. "In practice, it doesn't tend to scale past six [iSCSI arrays]," Foskett says, "but the first few scale nicely while giving you a lower price point to get into it."

SECURITY ISSUES

The biggest implementation differences involve security. Contrary to popular belief, Fibre Channel SANs are traditionally less secure than iSCSI SANs. The authentication protocols native to Fibre Channel are rarely used. Instead, most storage organizations rely on the fundamental differences in Fibre Channel fabrics and the complex nuances of LUN zoning and masking to keep SAN data secure. In fact, iSCSI actually has more security features than Fibre Channel. "From authentication to encryption, you find that iSCSI has many more options and that they're generally easier to use," Contoural's Foskett says. "But nobody is using them anyway."

In a Fibre Channel SAN, you must establish logical relationships (zones) that connect servers and storage, then block (mask) all but the authorized volumes on any given disk. By comparison, iSCSI doesn't use zoning. This is often perceived as a security problem, but iSCSI deals with "targets," so it's only necessary to mask targets. This means that a Fibre Channel SAN can see multiple LUNs on any particular disk, but iSCSI can only deal with a disk target. Consequently, iSCSI authentication is very important, and iSCSI employs advanced authentication methods to establish security, such as Challenge-Handshake Authentication Protocol (CHAP). "They use CHAP, which is just a much more secure method and it's really super simple to set up because people have been using CHAP in the IP world for a decade," Foskett says. Furthermore, Fibre Channel doesn't support native encryption over the wire, but iSCSI can utilize IPsec encryption to protect data in flight.

Experts agree that security is vastly improved by blocking off the SAN from the outside world. This was a natural element of Fibre Channel, but presents a challenge for Ethernet-based SANs—you don't want iSCSI SAN data leaking out over the user LAN. Building a different LAN and using it as a dedicated SAN may be the preferred tactic when the performance of iSCSI must be optimized. However, it is more common to establish an iSCSI SAN using a virtual LAN (VLAN) that carves up the physical LAN into a logical portion that is used exclusively by the SAN, allowing administrators to tightly regulate and guard the traffic that the VLAN carries.

Contrary to popular belief, Fibre Channel SANs are traditionally less secure than iSCSI SANs.

MIXING iSCSI AND FIBRE CHANNEL

For many organizations, the choice isn't Fibre Channel or iSCSI, but a mix of the two. Mixed SAN infrastructures have become popular because they preserve any existing Fibre Channel infrastructure while supporting the introduction and expansion of iSCSI in the enterprise. One example of this trend is "SAN inclusion," where secondary applications and servers that may have been too costly to place on the Fibre Channel SAN can now be interconnected into an iSCSI SAN. IT staff "might go back and say 'Look, we paid $50,000 for our Unix server, and we're paying $5,000 for Linux servers. Why don't we use iSCSI in that [low-cost] environment?'" Asaro says.

SANs can also be interconnected using an iSCSI gateway, a Fibre Channel switch with iSCSI support, intelligent storage switches and gateways, and multiprotocol storage arrays. iSCSI gateways are simple and unobtrusive (though they can be expensive). Gateways perform all of the translations between iSCSI and Fibre Channel. Examples of these iSCSI gateways include Brocade's iSCSI Gateway, Cisco's MDS 9216i and QLogic's SANbox 6140 Intelligent Storage Router.

Having iSCSI support in the Fibre Channel switch makes it easy to add intelligent features, like the Virtual Router Redundancy Protocol (VRRP) or iSCSI Server Load Balancing (iSLB). Such integration also offers a single management console with the redundancy and performance of an intelligent switch. For example, Brocade offers the Brocade FC4-16IP iSCSI Blade for its Brocade 48000 Director. Cisco provides the IP Storage Services Module and the Multiprotocol Services Module for its MDS 9200 Series Multilayer Fabric Switches and MDS 9500 Series Multilayer Directors.

iSCSI actually has more security features than Fibre Channel.

Intelligent storage switches and gateways add advanced storage services such as virtualization, snapshots, replication and mirroring. NetApp's V-Series gateways and the Sanrad iSCSI V-Switch are two examples of intelligent storage controllers with no storage attached, allowing for iSCSI, Fibre Channel and NAS connectivity to a storage pool. Multiprotocol arrays can also offer the same features but include storage in the same box. For example, EMC offers mixed protocol support in its Clariion CX3-20 and CX3-40 arrays, while Hewlett-Packard Co. supports iSCSI in its StorageWorks XP and EVA arrays.

Regardless of how you choose to merge Fibre Channel and iSCSI SANs, there should be no performance penalty on either side. But there is no performance guarantee, particularly in iSCSI deployment. For example, iSCSI target drivers can vary a great deal in their implementation, so some optimization may be required. The IT staff can help to analyze and optimize network performance for iSCSI.

WEIGHING iSCSI VS. FIBRE CHANNEL

Financial institutions, like Texas Trust Credit Union in Grand Prairie, TX, face the challenge of accommodating spiraling storage demands, especially with document images, while meeting retention and regulatory requirements. Their core business relies on an IBM P-series database and

application server running Unix with hundreds of gigabytes of internal storage. But there are other storage hogs to contend with. Microsoft Exchange for email and EMC Legato software for document management have swelled the credit union's total storage demand to about 2.5TB. "We see our storage needs in that area increasing for the next several years rather dramatically," says Boyce Crownover, system administrator at Texas Trust. Today, those applications are implemented on a modular NAS/iSCSI storage device running a custom Linux variant.

While the choice of iSCSI involved many parameters, Crownover cited compatibility and performance as the two most important criteria. Ethernet copper cabling was already installed in the infrastructure, supporting a wide range of Ethernet-based storage systems and simplifying the iSCSI installation. The choice of iSCSI also meant a more substantial role for network personnel, rather than strictly the storage professionals. More importantly, iSCSI presented adequate performance for running database and other applications. "iSCSI has the same availability as any NAS," Crownover says. "If we're using databases, which we do quite a bit, then we expect the iSCSI to pay off significantly over other file-level network types [NAS]."

> **"Honestly, if we had to put our primary database system on some sort of SAN, we might have gone Fibre anyway."**

There is always an element of uncertainty in any new technology deployment. The credit union's testing resources were limited, and Crownover's team visited sites with Fibre Channel, iSCSI and mixed infrastructures to determine the best fabric for its estimated throughput. "Honestly, if we had to put our primary database system on some sort of SAN, we might have gone Fibre anyway," Crownover says, noting that the disk storage already attached to the P-series provided adequate I/O capability. "We didn't have a need for anything [performance] that would exceed what we expected to get from iSCSI."

After three months in live production, Crownover said that there were no lingering issues. Any early concerns over the longevity of iSCSI have vanished as the industry continues to support iSCSI growth. "That was one of the factors for considering options besides Fibre," he says.

"The difference between TCP/IP vs. Fibre technology improvements over the last few years seems to have dramatically favored TCP/IP," Texas Trust's Crownover adds. The possibility of moving to 10 GbE is another advantage that weighed into iSCSI deployment.

Beyond Exchange servers and other everyday applications, civil engineering firms also face the challenge of storing large data-rich files and databases while ensuring adequate performance for application users. A typical AutoCad project might use files that are hundreds of megabytes in size, and this requires speedy but cost-effective storage. For the Timmons Group, a civil engineering and environmental design firm based in Richmond, Va., the answer came in an EMC Clariion CX3-20, which facilitates a mixed environment that supports 3TB of corporate storage across both Fibre Channel and iSCSI SANs.

The introduction of iSCSI into Timmons Group's storage environment has brought significant flexibility while maintaining cost effectiveness. "iSCSI allows us to be dynamic, because there's no cost for

Fibre Channel HBAs, it's just a NIC," says Bryan Moore, IT infrastructure manager with Timmons Group. "We just carve out a LUN on the back-end SAN and attach it via iSCSI. We can even get redundant with the iSCSI." That level of flexibility allows the organization to change as its clients' needs change.

Testing was limited, although Moore's team was able to run several iSCSI pilots to stress features like speed, redundancy and backup. "We found out that you can't do Fibre [Channel] and iSCSI on the same host," Moore says. "It was a good week's worth of piloting and testing with users." The testing process involved two dedicated engineers, but the mixed storage infrastructure was ultimately deployed to everyone's satisfaction.

Moore notes that Fibre Channel deployment wasn't terribly difficult, but ensuring the right firmware, hardware drivers, HBA emulator versions and other details could complicate HBA installation. Fibre Channel HBAs also need downtime for installation and configuration. By comparison, iSCSI deployment proved much easier. "Install Microsoft initiator tools, set some IPs with your NICs, carve out a LUN, and you're ready to go," Moore says. He is looking forward to migrating the iSCSI side of storage to 10 GbE. NIC and switch migration should be straightforward, as long as EMC follows through to provide a 10Gb iSCSI module for the CX3-20, which is currently expected.

> Regardless of how you choose to merge Fibre Channel and iSCSI SANs, there should be no performance penalty on either side.

THE FUTURE OF iSCSI AND FIBRE CHANNEL

There is no doubt that iSCSI has become the SAN of choice for mid-sized organizations. Even large enterprises are testing the waters with iSCSI deployments in workgroups or remote offices to gain a cost advantage. Asaro notes that international IT professionals with little, if any, Fibre Channel experience may leapfrog right over Fibre Channel to adopt iSCSI. However, nobody sees the end of Fibre Channel anytime soon. Few organizations are willing to discard their existing Fibre Channel infrastructure investment and experience base. "We expect to see more and more of a coexistence between them," Asaro says. "We expect that over time iSCSI will be the dominant SAN protocol, but it's probably going to take another three to five years for that to occur."

Virtual server deployment will be a catalyst for pervasive iSCSI storage networking in large and midsized organizations. "Once I do that, I'm going to put all of my VMware images, applications and data onto a storage network," Asaro says, citing a drive toward universal storage adoption with iSCSI between the virtual server systems and storage. ⊙

Stephen J. Bigelow is a features writer at TechTarget.

What's it like to feel 100% confident that your backup and restores will actually

work?

Visit the SearchStorage.com "Advanced Guide to Backup" today:

www.SearchStorage.com/backup_guide

Search**Storage**.com

The Web's best storage-specific information resource for enterprise IT professionals

iSCSI
case
studies

*Users praise their iSCSI SANs, citing
low cost, ease of use and
better-than-expected performance.*

By Deni Connor

P SAN ADOPTION IS GROWING among users who want storage that's
easy to install, configure and manage, and also comes at a price con-
siderably less than that of Fibre Channel SANs.

Consider Dave DePillis, manager of IT operations at Allied Cash Ad-
vance in Miami, who installed an iSCSI SAN (IP SAN) two years ago to
make use of the cabling, switches and network adapters installed in
his Gigabit Ethernet network. "Installing iSCSI was absolutely a no-
brainer, especially since I had such a small initial investment," says
DePillis. He's using iSCSI to back up file shares on four to six virtual
machines with Symantec Corp.'s Backup Exec 11 to a NetApp Inc.
FAS2020 file server. "I have more flexibility with iSCSI since I can use
my LAN switches," says DePillis.

James Santillo is another happy iSCSI user. "iSCSI is easy to use and
configure," says Santillo, systems administrator at Weiss Group Inc. in
Jupiter, FL. Santillo was able to implement iSCSI capability by installing
StorMagic's SM Series iSCSI software on some industry-standard
servers equipped with SATA drives.

JUST WHAT IS iSCSI?

iSCSI was adopted by businesses shortly after its ratification by the In-
ternet Engineering Task Force (IETF) in February 2003. The protocol, which
was developed within the IETF to transport SCSI commands and block-
level data over an IP network between a client and a target device, runs
on top of standard Ethernet adapters and over Ethernet LAN or WAN
switches.

The technology is implemented by loading a software-based driver—
called an initiator—on an Ethernet adapter or by adding a dedicated

iSCSI host bus adapter (HBA) to the host computer. Another initiator is added to the target storage array, which allows it to serve up data that will be transported across the network via the iSCSI transport.

iSCSI initiators are available from a number of sources and are categorized by operating system type. Two of the most popular drivers are a Windows initiator from Microsoft and a Linux initiator from SourceForge.

Target storage arrays are available from almost every storage vendor, including EMC Corp., NetApp and Overland Storage Inc. Target software—available from vendors such as FalconStor Software Inc., Open-E GmbH and StorMagic—lets users add to commodity servers or gray-box storage arrays from Intel Corp. to make them iSCSI-compatible so that they appear to the client as a local SCSI device.

iSCSI can also be implemented with gateway technology in which an iSCSI controller attaches to a block-level storage array, thus enabling iSCSI transport. Examples of gateway-enabled iSCSI products are available from Reldata Inc. and StoneFly Inc.

In addition, a number of vendors have joined the iSCSI and Fibre Channel worlds with what's called unified or multiprotocol storage. Vendors such as Microsoft, NetApp and Pillar Data Systems market arrays or software that can attach to the Ethernet network as a NAS or iSCSI device, and to the Fibre Channel SAN.

Businesses of various sizes have adopted iSCSI because it's easy to install, inexpensive, behaves just like Ethernet and doesn't require special skills like Fibre Channel does.

"We don't have Fibre Channel experience," says Scott Christiansen, IT director at Leo A. Daly, an architectural and engineering firm in Omaha, NE. "To get the iSCSI SAN up and running was so quick and easy, it was

iSCSI initiators

A number of vendors provide iSCSI initiators for most operating systems. Here's a sampling.

Vendor	OS support	Download site	Cost
Atto Technology Inc.	Mac	www.attotech.com/xtend.html	$195
Cisco Systems Inc.	Solaris	www.cisco.com/	Free
Hewlett-Packard Co.	HP-UX	www.hp.com	Free
IBM Corp.	AIX	Included with OS	Free
Microsoft Corp.	Windows	www.microsoft.com/	Free
Novell Inc.	NetWare	http://download.novell.com/Download?buildid=rIP6qIDo63s~	Free
Open-E GmbH	Linux	Included in software	N/A
SourceForge	Linux	http://sourceforge.net/project/showfiles.php?group_id=26396	Free
University of New Hampshire	Linux	http://unh-iscsi.sourceforge.net/	Free
VMware Inc.	VMware	www.vmware.com/	Free

SearchStorage.com | STORAGE

A sampling of iSCSI target devices

Vendor	Product	Max. raw capacity	Drive types: SATA, Fibre Channel (FC)
3PAR Inc.	InServ Storage Server	600TB	FC, low-cost FC
Adaptec Inc.	Snap Server 110; Snap Server 650, 520, 410 and 210	750GB; 36TB	SATA; SATA, SAS
BlueArc Corp.	Titan 1100, 2000 and 3000 Series	4PB	FC, SATA, WORM
Celeros Corp.	eXtremeSAN, EzSAN, EzNAS, EzSANFiler	96TB	SATA, SAS
Compellent Technologies	Storage Center	504TB	SATA, FC
Dell Inc.	AX4-5I	60TB	SATA, SAS
Dell EqualLogic	PS 5000	16TB	SATA
EMC Corp.	Clariion AX150i, CX300, CX500, CX700 and Celerra	336TB	SATA, SAS, Flash SSD
EMC	Symmetrix DMX	1PB	SATA, FC, Flash SSD
FalconStor Software Inc.	IPStor Enterprise Edition, Network Storage Server	250TB	SATA
Hewlett-Packard (HP) Co.	StorageWorks Enterprise Virtual Array; 1510i Modular Smart Array	240TB; 64TB	FC, low-cost FC; SATA, SAS
Hitachi Data Systems	Adaptable Modular Storage; Workgroup Modular Storage	320TB; 78.75TB	SATA; FC/SATA
Intransa Inc.	EdgeBlock, BuildingBlock, PerformanceBlock	1.5PB	SATA, SAS
Kano Technologies Corp.	NetCOR	51TB	SATA, SAS
LeftHand Networks Inc. (acquired by Hewlett-Packard)	Network Storage Modules; HP ProLiant DL320s; IBM x3650; Dell PowerEdge 2950	11.25TB/ module; 9TB; 1.8TB; 9TB	SATA; SAS/SATA: SAS/SATA; SAS
NetApp	FAS2000, FAS3000, FAS6000	1,100TB	SATA, SAS, FC
Nexsan Technologies Inc.	SATABeast, SATABeastXi, SATABoy	42TB per module	SATA
Open-E GmbH	iSCSI-R3 (software); Data Storage Server (DSS)	N/A	N/A
Overland Storage Inc.	REO 1500, 4500, 4500c, 9100, 9100c	18TB	SATA, SAS
Pillar Data Systems	Axiom 300, 500	832TB	SATA, FC
Pivot3 Inc.	RAIGE Storage Cluster	9TB per module	SATA
Reldata Inc.	Unified Storage Systems	N/A	SATA, SAS, FC
StoneFly Inc.	OptiSAN, Hybrid Storage Concentrators, Integrated Storage Concentrators	300TB	SATA, SAS
StoreVault, a division of NetApp	S300; S550	6TB; 12TB	SATA; SATA
StorMagic	SM Series (software)	N/A	N/A

STORAGE
SearchStorage.com

Vendor resources

iSCSI security

iSCSI case studies

iSCSI vs. FC

iSCSI and VMware

just unbelievable." Christiansen adds that the SAN "uses the same media as the Ethernet network; it's nice in the sense that everything we buy is Category 6 cable—it works for Ethernet, it works for the IP SAN."

APPLICATIONS RUNNING ON ISCSI

A few years ago, many analysts predicted that Fibre Channel SANs would be reserved for business-critical applications such as transactional databases, while iSCSI would be deployed for less business-critical, front-office applications, file shares and Web services. But when talking to users from various-sized organizations, it's clear that iSCSI deployments span mission-critical applications and less-demanding office applications.

"Our primary business app runs off a Microsoft SQL Server," says Mike Leather, network services manager at Safeway Insurance Group in Westmont, IL. "Our developers and database administrators were telling me that our disk I/O performance wasn't acceptable—that was because we were growing too big for the original solution [and] we needed to look at something else."

Leather looked at Fibre Channel SAN storage, but was wary of the challenges and expenses involved. He installed an IP SAN from EqualLogic (now owned by Dell Inc.) primarily for his SQL Server environment, but soon found he was using iSCSI for everything. "The whole thing started out for SQL Server and exploded," he says. "We are using the SAN for file storage, Exchange servers and our VMware environment."

> "Our primary business app runs off a Microsoft SQL Server."

Weiss Group's Santillo found that iSCSI will support all of his applications, whether they're business-critical or not. "Our custom in-house CRM app, which was running on Fibre Channel, is now being moved to iSCSI," he says. "We had six SQL Server apps on Fibre Channel, but [they] are now on iSCSI. And we're moving our two Exchange databases to iSCSI. The CRM app is going on the Xiotech box [which is iSCSI-enabled]. We're also moving our file systems and unstructured data over to Xiotech," he says. "I needed enterprise-level reliability without the price." Santillo says his six-year-old IBM Fibre Channel SAN will become "end-of-lifed. We're migrating everything off to iSCSI."

iSCSI INITIATORS

In the early days of iSCSI deployments, almost no one expected iSCSI software initiators to prevail over dedicated iSCSI HBAs. Adaptec Inc., Alacritech Inc. and QLogic Corp. originally marketed iSCSI adapters complete with features such as TCP Offload, which negates some of the overhead of TCP/IP. These adapters were expensive and often sold for as much as $750, which is four to five times the cost of standard Ethernet adapters.

"We use the VMware and Microsoft iSCSI [Software] Initiator, and we also use iSCSI and Fibre Channel HBAs from QLogic," says Chris Rima, IT systems supervisor at UniSource Energy Corp. in Tucson, AZ. "We've been decreasing the use of the Microsoft iSCSI Initiator because it's not as efficient as the VMware iSCSI initiator or the QLogic iSCSI HBAs.

There's a higher cost associated with the QLogic HBA, but it's minimal compared to the performance gains we get."

But other users have overwhelmingly adopted the use of software initiators from Cisco Systems Inc., Microsoft and the open-source community because they're inexpensive or even downloadable for free from a vendor's site.

"We use the Microsoft software initiator and it works fine," says Mark Kash, IT specialist for the U.S. Army Corps of Engineers in Huntington, WV. "It's reliable and I haven't had any instances where it's corrupted anything," he says. "Originally, we considered using TOE cards from QLogic because we were thinking a firmware-based platform may be more reliable, but we saved money using the software-based alternative."

Microsoft's iSCSI Software Initiator Version 2.07 is the most popular iSCSI initiator. It supports multipathing for load balancing and failover, 64-bit platforms and IPv6. Multipathing lets the initiator establish multiple sessions with one target, enabling load balancing and failover among multiple network adapters or HBAs.

IS PERFORMANCE GOOD ENOUGH?

According to analysts, iSCSI performance would fall short of Fibre Channel. However, end-user experiences don't bear that out. "We ran some performance tests to see the difference between Fibre Channel and iSCSI, and we saw what the industry saw: iSCSI is able to offer about 80% the performance of 2Gb Fibre Channel," says UniSource Energy's Rima. "4Gig Fibre Channel is a little bit more, but it's not substantial enough given the cost to use it."

Rima said he chose iSCSI because it fulfilled his need for performance. He runs Microsoft Exchange on iSCSI, and has been able to scale his storage up but "maintain a network topology that's low-cost and low-impact in terms of support."

Jim Bollinger, systems and network engineer at Washington and Lee University in Lexington, VA, has seen the same performance results as Rima. Bollinger installed Overland Storage REO disk-based appliances to back up his storage environment.

"iSCSI has been capable of doing everything we need it to do," says Bollinger. "You could take iometer.exe and take the array right up to 100MB/sec. It's every bit as good as local SCSI and sometimes better. We've had no trouble on big files filling the pipe on our LTO-3 backup—up around 70MB/sec to 80MB/sec—and we've been backing up 7TB to 8TB a day."

$2,000,000,000

ACCORDING TO STAMFORD, CT-based market research group Gartner Inc., iSCSI is expected to be a $2 billion market by 2010. In addition, IDC estimates that from now through 2010, iSCSI SANs will show a compound annual growth rate of 74.8% for worldwide revenue vs. 4.1% for Fibre Channel. IDC also claims the iSCSI protocol will capture more than 10% of storage systems revenue and an even greater percentage of capacity by 2008.

10Gb/SEC ETHERNET

The advent of 10Gb/sec Ethernet bodes well for iSCSI. With Dynamic TCP Offload added to 10Gb/sec adapters running iSCSI, users will see the benefits—higher performance and access—of removing TCP processing from the host computer and placing it on a dedicated HBA from vendors such as Alacritech, Neterion Inc. and NetXen Inc. Dynamic TCP Offload takes advantage of Microsoft's TCP Chimney Offload technology, which offloads the TCP stack to the network card.

Bollinger, who uses QLogic HBAs that perform both TCP and iSCSI offload, says he'll migrate to 10Gb/sec Ethernet for the trunks between university buildings.

"10Gb/sec to 100Gb/sec is in our planning process and further validates our decision to deploy iSCSI," says Kash with the U.S. Army Corps of Engineers. He adds, "I'm comfortable that iSCSI is going to take over from Fibre Channel, and [that] it will no longer be considered a low-cost, lower performing alternative."

Rima says, "We can do TCP Offload with the TCP Offload on our NetApp boxes," adding that "10Gig should allow us to scale up quite a bit."

Besides being able to use existing Ethernet switches, adapters and common Category 6 cabling, iSCSI users have seen other advantages.

According to analysts, iSCSI performance would fall short of Fibre Channel. However, end-user experiences don't bear that out.

"The ROI of iSCSI is hard to measure, but our complaints from users on performance issues are practically non-existent now," says Safeway Insurance Group's Leather. "That's a huge ROI. In our business, if someone has trouble with our Web site while they're writing insurance, they won't wait for us, they'll just go to the next insurance carrier. You can't measure the lost business." ⊙

Deni Connor is principal analyst at Storage Strategies Now (SSG-NOW.COM), an IT research firm based in Austin, TX.

iSCSI

security

With a little planning, your iSCSI storage network can be even more secure than a legacy Fibre Channel storage network.

By Stephen Foskett

F YOU'RE THINKING ABOUT implementing an iSCSI storage network, as sure as the sun sets each day, someone will ask about security. Here's the short answer: iSCSI can be as secure as you want it to be.

"Now that storage is being put back on Ethernet and IP networks, customers are becoming concerned about access control and encryption," says Kyle Fitze, marketing director for Hewlett-Packard Co. SANs, StorageWorks Division. The commodity protocols and hardware used in iSCSI networks can, in theory, connect to just about any computer, from a rack-mounted server to a laptop or handheld PC. iSCSI was built from the ground up with strong authentication and encryption capabilities . . . as long as they're used.

So if iSCSI has so many security features, why do so many people ask about security? The reason is that iSCSI is much more accessible than previous storage protocols. Ethernet hardware and IP support have become ubiquitous, both inside and outside the data center. The technology uses common protocols and is supported by the majority of OSes available today. This means there are millions of people who could theoretically try their hand at breaking into an iSCSI SAN.

This accessibility is also a blessing for iSCSI. On the positive side, there's a lot more understanding and acceptance of its basic concepts vs. Fibre Channel. There's also a legion of trained network engineers who have the skills to build a secure network for iSCSI to run on. Technologies like Challenge-Handshake Authentication Protocol (CHAP), Remote Authentication Dial-In User Service (RADIUS), VPN and IPsec have proven to be powerful and reliable over a decade of widespread use.

This stands in contrast to the arcane security features, most of which are rarely used, offered by Fibre Channel storage device vendors. "Our iSCSI SAN is definitely more secure because of our previous experience with IP and Ethernet," says Ron Braden, IT director for the Town of Vail, CO. "Building a secure IP network is second nature to us."

A secure system addresses data confidentiality, integrity and availability. Most people begin with confidentiality. But availability is equally important and probably accounts for more security breaches. A denial-of-service attack is much simpler to engineer than an encryption hack. Data can also be deleted, requiring time-consuming restores.

Integrity is a more subtle topic. Substituting bad data for good can go unnoticed and could lead to more serious side effects than losing access to a system. Problems with integrity can lead to legal and compliance issues that are more costly than any technical problem.

ISOLATE THE iSCSI NETWORK

The most important step in building a stable and secure iSCSI SAN is to keep it separate from other networks (see "What to do first," this page). "We were not as worried about security as about denial of service," says the Town of Vail's Braden. "It was too risky from a performance standpoint to allow storage traffic to share the network with other applications." Braden's iSCSI SAN contains what's called an "air gap," which contains dedicated Ethernet switches and isolated fiber-optic cables for storage. This approach reduces the risk that a problem on the main data network would overflow into the SAN. Each

---

What to do first

Experts agree that there are certain things everyone using iSCSI technology should do:

▶ Deploy iSCSI on a secure, isolated virtual LAN (VLAN) or subnet that doesn't route outside the data center.

▶ Keep management interfaces on a secure network.

▶ Use role-based access control and keep a log of all management activities.

▶ Use encryption anytime iSCSI traffic leaves a secure network (e.g., WAN connections).

▶ Employ Diffie-Hellman Challenge-Handshake Authentication Protocol (DH-CHAP) to authenticate servers and storage arrays to each other.

▶ Employ security technologies that are appropriate to your business without going overboard on complexity—sometimes simpler is better.

of Vail's SAN-attached servers has two Ethernet interfaces: one for the SAN and one for the LAN.

A larger iSCSI implementation at an international bank was configured similarly. Routers and switch configuration throughout the network prevented iSCSI data from leaking from one network segment to another. And the bank used iSCSI host bus adapters (HBAs) instead of standard Ethernet cards. The HBAs it chose couldn't be configured to carry general network traffic, which reduced the risk of an intruder using the iSCSI SAN as a "bridge" to other secure networks.

WHO ARE YOU?

There are many ways to authenticate a person before granting them access to the iSCSI SAN. You can authenticate based on who someone claims they are by requiring positive identification before talking to them or by continually checking their identity as long as they're connected.

Borrowing a concept from Fibre Channel, most iSCSI arrays allow you to control access based on a unique identifier for each attached client. While Fibre Channel uses a WWN for LUN masking, iSCSI can use an IP address, a MAC address or a unique name assigned to the iSCSI initiator software running on the client to hide targets. Although none of these methods is very secure, they do protect against accidents on the part of storage admins. Plus, some iSCSI initiators have been known to "grab" all the storage they can see, making masking a requirement. All of these values can be easily changed in software, so spoofing them is trivial.

If masking iSCSI targets isn't enough, CHAP adds another layer of security. The common authentication protocol in IP circles, CHAP uses public key encryption concepts to verify the identity of connected devices. It validates that both devices know a "shared secret" like a password, making it harder to gain access to the storage array. "The iSCSI standard requires that all iSCSI initiators and targets include CHAP support, but not all customers choose to turn it on," reports Eric Schott, director of product management at Dell/EqualLogic Inc.

CHAP can also be used to authenticate the array to the clients. John Spiers, founder and CTO of LeftHand Networks (since acquired by Hewlett-Packard), recommends that all iSCSI users implement two-way CHAP, also known as Diffie-Hellman CHAP (DH-CHAP). "A single-way CHAP session could be spoofed to break in or set up a man-in-the-middle [attack]," says Spiers. "DH-CHAP is much more secure."

But CHAP isn't totally secure. "CHAP is subject to offline dictionary attacks—the secret can be guessed with a powerful computer," admits Alan Warwick, lead software design engineer for iSCSI at Microsoft Corp. However, this would be time-consuming and difficult, because a CHAP login would have to be captured by a network sniffer situated on the storage network. Warwick suggests that administrators concerned about the possibility of a CHAP attack use 16-byte secrets and change them frequently.

> Some iSCSI initiators have been known to "grab" all the storage they can see, making masking a requirement.

The most secure option for authentication is IPsec Authentication Header (AH), which has a digital signature on every packet. Unlike a full implementation of IPsec that encrypts the entire packet, IPsec AH merely authenticates the sender, recipient and checksum for the message content. This effectively authenticates the entire message, but does nothing to protect its content from snooping. Although there's still some performance impact, it's much easier to encrypt a 60-byte header than a 64KB packet.

SNOOPING iSCSI PACKETS

Snooping the contents of iSCSI packets, one of the first threats people mention when asked about iSCSI security issues, is less likely to occur than other types of attacks. An IP SAN with no security controls will probably run on a switched Ethernet network. Switches create point-to-point paths for data, so each port sees only the traffic intended for it. To snoop on iSCSI traffic requires some sort of advanced sniffer function to send all traffic to your port, which would require administrative access to the Ethernet switch.

There are many options to protect data in motion over the network.

A more secure iSCSI on the way

▶ **Hardware–accelerated IPsec.** Changes are coming that will make iSCSI even more secure. Vendors say that hardware-accelerated IPsec will be a common feature in iSCSI initiators and storage arrays within two years. "Today's CPUs can keep up encryption processing at gigabit speeds, but 10Gb Ethernet will change all of that," says John Matze, president and CEO of Siafu Software LLC, and one of the original authors of the iSCSI protocol. He expects encryption processing will move to routers or storage arrays to provide wire speed throughput at 10Gb/sec.

▶ **Microsoft's iSCSI Software Target.** As Microsoft's market share of the entry-level iSCSI market grows, it will become easier to implement security technologies through its iSCSI target software, which can be configured using the same group policy editor that controls the configuration of Windows servers and desktops. Many iSCSI arrays also integrate smoothly with Windows domains for management authentication.

▶ **Trusted Platform Module.** Changes in server architectures also have implications for iSCSI. A Trusted Platform Module (TPM) is a specialized chip that can be installed on the motherboard of a PC or server to authenticate the computer rather than the user. To do so, TPM stores information specific to the host system, such as encryption keys, digital certificates and passwords. TPM minimizes the risk that data on the computer will be compromised by physical theft or an external attack. TPM chips are expected to spread to disk drives and storage systems. While the TPM wouldn't eliminate the need for any of the current encryption or authentication techniques, it would make data stored on storage arrays even more secure.

For example, IPsec Encapsulating Security Payload provides advanced authentication of each packet, effectively eliminating the possibility that someone could read data while it travels across the network. And if stronger encryption is required, it's possible to replace the standard encryption protocols used by IPsec with a more powerful alternative.

Another option is to use an encrypting file system on the server to encrypt data before it gets to the IP SAN. This encrypts data in motion as well as data at rest because no data leaves the server unencrypted. It also prevents all sorts of man-in-the-middle attacks on the network because any tampering with the content interferes with the server's ability to read the data. The downside of using an encrypting file system is the impact it can have on server performance. Even a powerful server can see a noticeable performance hit when using this type of encryption technology.

A VPN creates a point-to-point encrypted tunnel between secure networks. The use of VPN technology should be a requirement whenever sensitive data travels across an uncontrolled network. The Town of Vail relies on an encrypted VPN tunnel for replication to a disaster recovery site, leveraging an existing WAN connection for its daily synchronization.

MANAGING MANAGEMENT

Probably the most vulnerable point in an iSCSI network has nothing to do with iSCSI at all. Nearly every network device can be managed remotely over a network. This management traffic can travel in-band (sharing the same network as the data) or out-of-band (using a dedicated network). Almost all storage devices, including Fibre Channel, SAN and iSCSI arrays, have management ports that operate using Eth-

Regulations drive security concerns

Much of the concern over data security in IP circles is driven by government regulations. On the business side, an equal concern is the threat of litigation. Perhaps the regulation that is most frequently cited is the Sarbanes-Oxley (SOX) Act of 2002, which requires that certain financial data have an audit trail back to its source. But SOX is only the tip of the iceberg. California's Information Practices Act, also known as SB-1386, has broad implications. It requires companies that have experienced theft of personal information data to notify any customers who might be potentially affected. SB-1386 has driven many companies to implement encryption so they can protect their customers' private data.

The Graham-Leach-Bliley Act of 1999 and HIPAA also require companies to protect personal data. In addition, the Payment Card Industry (PCI) Data Security Standard has strict requirements for credit card processors. Companies affected by any of these regulations should strongly consider encryption technology and should assess whether their storage networks are vulnerable to data theft.

ernet and IP. In nearly all cases, these management ports are the easiest way to hack into the storage array.

Many management interfaces support outdated or insecure protocols like SNMP, Telnet and HTTP, as well as more secure protocols like Java and HTTPS or SSL. These older protocols can often be exploited for destructive purposes, allowing an attacker to access confidential configuration information or even bring down the array. This is especially true if default user names and passwords aren't changed when systems are configured. Some systems also have default accounts for vendor service, which can be the same across an entire region or even a company's whole product line. These accounts can be especially destructive because they often yield access to diagnostics areas and configuration information.

Probably the most vulnerable point in an iSCSI network has nothing to do with iSCSI at all.

For this reason, management interfaces must be treated just like data interfaces and placed on isolated nonrouting subnets with firewalls and VPNs to prevent unauthorized access. Unfortunately, this is not standard practice. In most sites, management interfaces are connected to the main corporate network and left open. The Town of Vail's Braden runs the management application on a server with one network interface card on the SAN and one on the LAN, and uses a remote desktop to access it securely.

REALITY CHECK
It's important to remember that the stereotypical teenage hacker attacking your systems from across the Internet reflects only a small portion of actual security breaches. You're far more likely to suffer a breach in the confidentiality, availability or integrity of your data at the hands of an insider, whether malicious or not.

There have been numerous press reports of insiders who have absconded with critical data and it's likely there are exponentially more cases that go unreported. Preventing unauthorized employee access to data has become more critical in light of regulations like the Sarbanes-Oxley Act of 2002, HIPAA and the Payment Card Industry Data Security Standard (see "Regulations drive security concerns," p. 26). Sadly, no current IT technology allows storage managers to understand the importance of the data contained in the bits and bytes they manage. Enabling this kind of security will require a whole new level of interaction between IT and business units.

Not all security breaches are malicious. Many common breaches are accidental or caused by an interaction of unrelated system components. For instance, a system admin could take down a RADIUS server, not realizing that it was authenticating storage traffic. Or a backup administrator could restore all files in a directory instead of just the requested one.

A final element to consider is that storage is one of the lower-level slices of the IT systems layer cake. No matter how secure your storage array and network are, data will always be vulnerable if a server or app is compromised. "The focus today is more on securing your servers—if you have access to the server, then you have access to the storage,"

says LeftHand Networks' Spiers. No amount of encryption or authentication will prevent access by a program or user who's supposed to get in. In the end, all storage admins can do is keep their system reliable and hope others do the same. ⊙

Stephen Foskett is director of Contoural's Data Practice. He has authored numerous articles and is a frequent presenter at industry events.

Check out the following resources from our sponsor:

Double-Take Software

netBoot/i Product Page

sanFly Product Page

Press Release

More Functionality, Less Infrastructure: Managed It With netBoot/i

About Double-Take Software

Double-Take® Software is the standard in data protection for Microsoft® Windows® applications and provides accessible and affordable data replication and failover solutions for disaster recovery, high availability and centralized backup. With its partner programs and professional services, Double-Take Software is the solution of choice for over ten thousand customers, from SMEs to the Fortune 500, in the banking, finance, legal, retail, manufacturing, government, education and healthcare markets. For more information, please visit www.doubletake.com.