

Indus Corporation

Improving a Key Federal Agency's Disaster Recovery Metrics by More Than 90 Percent with Symantec Solutions



In the wake of 9/11, a federal agency critical to the country's security needed to ensure business continuity if the nation's capital encountered an attack or disaster. Symantec Business Partner Indus Corporation provided the agency with a Veritas Storage Foundation *for Windows* Disaster Recovery solution, enabling an innovative, A to B to C recovery-site design that maximized its flexibility of response, while reducing the time needed to recover by over 90 percent with data loss to near zero.

Organization Profile

A federal agency, key to the country's security, needed a way to ensure business continuity of its business-critical email application.

Industry

Government

Solution

Data Protection
Disaster Recovery
Business Continuity

Continuity meets catastrophe

For government agencies, business continuity has always been critically important. But the events of September 11, 2001 and the devastation in the wake of Hurricane Katrina in 2005 made the need to protect data, ensure application availability, and enable agencies to continue to function in the event of a significant disaster all the more apparent.

The IT team at one government agency knew its existing disaster-recovery plan wouldn't provide sufficient protection in the event of a catastrophe. The agency relied on a single data center to support its mission-critical email application, and manually backed up its data to tape daily to provide data protection. If the data center went down, it typically took 72 hours to restore the servers and get it up and running again. And if the tape backup failed, or the tape was damaged or lost, as much as 24 hours' worth of critical information could be unrecoverable, lost forever.

Changing the definition of DR

"September 11th changed a lot of things," recalls Charles Bost, senior systems engineer with Indus Corporation, the company hired by the agency to manage its data center. "It certainly changed the agency's disaster recovery scope, and what we wanted to accomplish. And then a mandate came down that the email servers had to stay up no matter what. That's not surprising, because email is the lifeline of this organization."

Bost, who is responsible for managing the agency's 1,300 email accounts, was charged with coming up with a solution. "The two-node, single data center solution we had in place wasn't going to provide that kind of availability," he explains. "Typically, if that data center went down, it could take us as much as 72 hours to become operational."

In response, Bost and his team designed a three-site, disaster-recovery plan that would allow the agency to stay up and running under almost any foreseeable circumstance.

"Our main objective was flexibility. None of the other solutions we considered gave us the flexibility of the Symantec solution."

Charles Bost

Senior Systems Engineer
Indus Corporation

Symantec and Indus Corporation help a federal agency ensure business continuity even in the event of a crippling disaster.

Flexibility fosters continuity

“Our main objective was flexibility,” Bost explains. “If the agency's main data center went down, we wanted to fail over to a 'hot' site a few miles away. That way, if we had a power failure at the main site, agency employees could simply continue working from systems based at the secondary site.”

But that solution alone didn't offer protection against a significant disaster. “That's when we decided to throw a third site in the mix,” says Bost. “In the event of a true disaster, where we lost both the primary and the secondary site, we could fail over to our third site located 50 miles away.”

The plan was solid. The next step was to find the software that could support it.

Ingenuity requires innovation

The agency's former solution wasn't up to the task: Although it could support the stretch cluster, it could only support a single node at each location, which didn't give the agency the failover flexibility it was hoping to achieve. Bost and his team then looked at another product, which initially looked promising, but ultimately couldn't support the number of nodes the agency intended to deploy either.

They decided that only a solution from Symantec—Veritas Storage Foundation for Windows Disaster Recovery (DR)—could provide the application availability and data protection the agency required. Veritas Storage Foundation for Windows DR includes Storage Foundation for Windows, Veritas Cluster Server with the Global Cluster Option, and Veritas Volume Replicator.

“Not only could the Veritas solution support the stretch-cluster arrangement, with Veritas, we could support as many as 32 nodes at each location,” says Bost. “None of the other solutions we considered gave us the flexibility of the Symantec solution.”

Spanning the distance

Though the number of nodes to be supported presented an insurmountable problem for other solutions, Veritas Storage Foundation for Windows DR could easily support the nine-node, three-site solution the agency wanted to deploy.

By replicating data asynchronously to the remote sites, the agency was able to virtually eliminate data loss resulting from unplanned data center downtime or failure, and reduce the recovery time objective (RTO) by 96 percent from three days to just a few minutes.

In addition, the Symantec solution lets the agency IT team fail over from the main data center to either remote site with a single mouse click, completing the operation in only five to 10 minutes, rather than the one hour it previously took.

Improved manageability

Veritas Cluster Server combined with the Global Cluster Option provides high availability by allowing IT staff to monitor proactively the health and performance of critical data center applications at the secondary and tertiary data centers that are nearly 50 miles apart. “In addition,” says Bost, “the Global Cluster Option allows us to failover the entire system to either of the DR sites, quickly and easily. In fact, because we're operating in cache mode, the whole process is pretty much transparent to the users. They wouldn't notice any difference in performance.”

The agency chose the Veritas Cluster Server Enterprise Agent for Exchange to keep Microsoft Exchange highly available, as it detects any failures and automatically brings the application online again.

Veritas Volume Replicator reduces data loss and shortens the agency's recovery time by allowing data to be replicated over IP among dissimilar storage devices. The solution's FlashSnap feature enables nearly instantaneous recovery of a downed server, compared to the six hours previously required to reconfigure a server from tape backups.

“We'll be using FlashSnap to take snapshots of our server setups following a backup,” explains Bost. “This will enable us to perform nearly instantaneous restores.”

Flexibility means savings—in time and money

In addition, the Volume Manager component of Veritas Storage Foundation allows storage in the agency's storage area network (SAN) to be virtualized. Physical disks can be grouped into logical volumes, allowing IT to configure, share, and manage the agency's existing storage to achieve optimal capacity—without taking applications down.

“The dynamic disk feature of Storage Foundation allows us to allocate as much disk space in the SAN as we need, whenever we need it,” explains Bost. “That's been a tremendous benefit to us. If we still had the other clustering solution, we'd have had to take the application offline, reallocate the storage, and then reload all the required data—a process that could easily take a couple of hours. Today, we can accomplish this in a matter of minutes.”

As a result, “We're looking at increasing the size of the agency's user mailbox quotas above 50 MB for 1,300 users by carving available space out of our SAN and giving it to our Microsoft Exchange information stores. And thanks to the Storage Foundation wizards, I can get it done with a few clicks, and no downtime,” Bost says.

SOLUTION AT A GLANCE

Business Drivers

- Ensure protection of critical data and applications in the event of a disaster
- Eliminate data loss during failover to secondary or tertiary site
- Improve storage utilization to accommodate data growth

Technology Challenges

- Establish a synchronous three-site, disaster-recovery solution
- Ensure that critical data is mirrored to each DR site
- Enable failover to remote, tertiary DR site in the event of significant disaster affecting primary and secondary sites
- Improve application availability from 99% to 99.99%, as mandated by agency administration

Solution

Enable an innovative and synchronized disaster-recovery solution at three sites

Symantec Products

- Veritas Storage Foundation™ DR for Windows consisting of:
 - Storage Foundation HA for Windows (includes Storage Foundation plus Veritas Cluster Server for Windows)
 - FlashSnap Option
 - Veritas™ Volume Replicator
 - Global Cluster Option
 - Veritas™ Cluster Server Enterprise Agent for Exchange

Technology Environment

- **Applications:** Microsoft Exchange 2003
- **Server Platform:** Nine HP ProLiant DL380 G3s running Microsoft Windows Exchange Server 2003
- **Storage:** Three HP StorageWorks MA 8000 Modular SAN Array with an HSG80 controller
- **Tape Library:** HP MSL 4026S2 Tape Drive Library

Symantec Services

- Symantec Technical Support (Extended)

Symantec Partner

- Indus Corporation

Because the Symantec solution is vendor neutral, Bost can shop around for the hardware solutions that make the most sense for the agency. “We're not locked in to any particular vendor with this solution,” he explains. “We can look at all the options on the market and choose the one that best fits our environment.”

“The Global Cluster Option allows us to fail the entire system over to either of the DR sites, quickly and easily. In fact, because we're operating in cache mode, the whole process is pretty much transparent to our users. They wouldn't notice any difference in performance.”

Charles Bost
Senior Systems Engineer
Indus Corporation

A solution that works, seamlessly

Bost says the agency recently had the opportunity to test the solution when the air conditioning at the agency's primary data center failed.

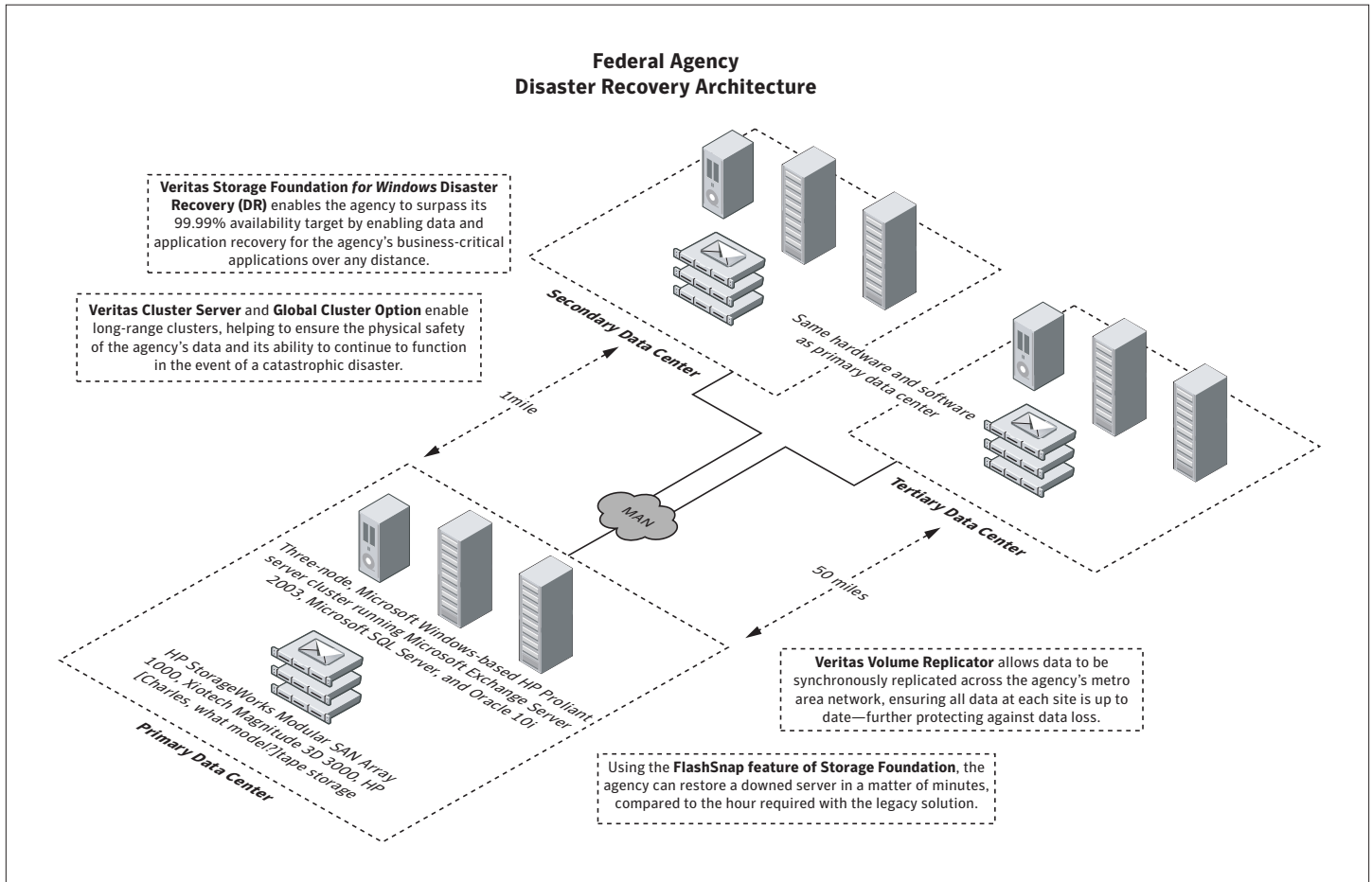
"I got a call letting me know that the power had to be shut off at the main data center, along with a request to failover to the secondary center. We were up and running from the secondary site in about 15 minutes," he says. "That's compared to the six or seven hours we probably would have been down with our legacy solution."

In another example, the agency's secondary site was recently threatened by flooding. "We actually had to unplug equipment and move it up a few floors to protect it," Bost recalls. Without the flexibility offered by the third site, "We would have once again been vulnerable to downtime through having a single point of failure."

Pushing the envelope together

Extended, 24x7 Symantec Technical Support has proven particularly useful for Bost and his team. "Just the other night, I was doing some work on the secondary site and was on the phone at one in the morning, talking to a Symantec support engineer in Australia who walked me through my task. Extended support gives us the flexibility we want.

"Symantec support has been excellent. We are extremely happy with what the Symantec team has done for us. We were pushing the envelope with this three-site solution design, and they kept coming back with what we needed as we tested it and put it into production. With the flooding we recently had, other government agencies like ours are taking a keen interest in what we've done here.



BUSINESS VALUE AND TECHNICAL BENEFITS

System Availability

- 99.99% availability target surpassed
- 96% reduction in unplanned downtime (6 hours to 15 minutes)
- 96% reduction in recovery time objective (RTO, 72 hours to 3 hours)
- 92% reduction in time to restore server (1 hour to 5 minutes)
- Planned storage-maintenance downtime eliminated because of ability to change storage allocation on the fly

Data Protection

- Recovery Point Objective (RPO) effectively reduced to zero (network latency)

Operational Efficiency/Savings

- 96% reduction in time to administer storage space (2 hours to 5 minutes)
- Vendor neutrality enables cost-efficient expansion of data center and storage environment
- Ability to reallocate storage resources without incurring downtime

“Symantec has the best solution out there. We thought so when we first started looking into DR solutions for our data center and we think so today. It's just a great product.”

Charles Bost

Senior Systems Engineer
Indus Corporation

“We think Symantec has the best solution out there,” Bost sums up. “We thought so when we first started looking into DR solutions for our data center and we think so today. It's just a great product.”

Today, should disaster strike—even disaster on the magnitude of a terrorist attack or a Category 5 hurricane—this government agency will stay up and running and doing the people's business, thanks to the power of its Symantec solutions. ■