



“ For over a decade Coolspirit have been supplying the UK’s top organisations with storage products and solutions so be assured we will meet your requirements head on.

It’s all about getting things right first time, quickly and simply! ”

Damon Robertson
Coolspirit Ltd

Our address

24 The Bridge Business Centre
Beresford Way
Chesterfield
S41 9FG

Get in touch

Call us on: 01246 454222
Email us: web@coolspirit.co.uk
Find us: [View location map](#)
Web: www.coolspirit.co.uk

Office hours

mon - thurs 8:30am - 5:30pm
fri 8:30am - 5pm
sat - sun Closed

“ Boost your storage buying power...
use ours! ”

Buy with confidence from
Coolspirit your authorised
Dot Hill Partner



Dot Hill AssuredUVS™

Unified Virtual Storage

Data Protection Technologies

Eight Ways to Evaluate Business Continuance Strategies



Copyright © 2010 Dot Hill Systems Inc. All rights reserved. AssuredUVS, Dot Hill, and the Dot Hill logo are trademarks of Dot Hill Systems Inc.

Other company and brand products and service names are trademarks or registered trademarks of their respective holders.

Part Number 540009-23b
December 16, 2010

Business Continuity: The Business of Ensuring 'Business as Usual'

Disasters happen and will continue to do so. Stark images of the latest devastating hurricane, tornado, tsunami or terrorist attack demonstrate widespread destruction and human suffering. Less reported but no less real are the thousands of businesses unable to maintain critical business operations after a disaster strikes. As a result, surveys find that over half of such businesses typically never reopen. For those that do, the large majority end up closing within two years of the original disaster.¹ For many businesses, even as little as an hour of downtime can translate to between several hundred thousand and several million dollars of lost revenue, as shown in the following figure.²

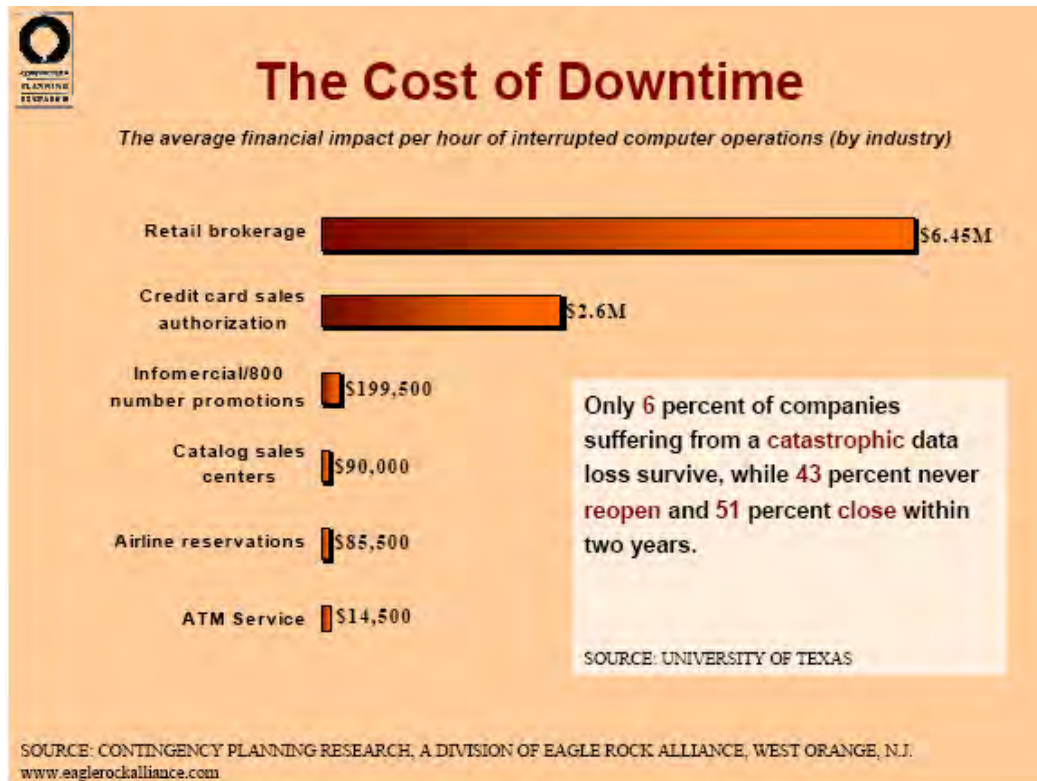


Figure 1. The Business Cost of an Hour of Downtime.

Such drastic examples of disaster serve as a ready reminder for business executives and their IT counterparts that no company is immune from the human and monetary impact of a potentially serious business disruption. Surprisingly, such catastrophic events comprise a small percentage of the overall reasons a company's critical operations and systems could be interrupted. Far more likely are disruptions due to localized failures such as temporary power outages, a component or network system failure, problematic system upgrades, complex technology refreshes, or computer viruses that cause rolling disasters and leave trails of corrupted data behind them.

From an IT perspective, the job of adequately protecting and quickly restoring a company's critical systems and data usually falls to already taxed IT groups. To help them, many such groups have begun to develop their own business continuity (BC) and disaster recovery (DR) plans and processes. These tend to combine the latest best practices with emerging BC technologies in order to achieve rapid restoration and continued high availability of their primary, production systems--regardless of the type of disruption.

¹ "Phoenix Disaster Recovery Newsletter," Issue 43, by Binomial International, a New York- and Canada-based disaster recovery and business continuity consulting firm, <http://www.binomial.com/newsletter/newsletter.php?issue=43>.

² Statistics from Contingency Planning Research, a division of Eagle Rock Alliance, West Orange, N.J., <http://www.eaglerockalliance.com/>.

Driven by company-wide initiatives and efforts to comply with government regulations surrounding the storage, retention and availability of a company's critical data, such BC plans often encompass three areas:

1. Disaster risk identification and business impact analysis
2. Risk avoidance/risk mitigation strategies
3. Disaster response strategies that minimize the impact of a given disaster on business operations

Despite these efforts, many IT organizations find themselves sorting through a dizzying, and often costly, range of technical solutions that claim to answer all of a company's needs for business continuance or disaster recovery. What these organizations really require is a simple way to evaluate and assess the various BC/DR solutions, and determine the right mix of cost and functionality for their needs.

This white paper addresses the issue by first taking a holistic view of the various facets of business continuance needing to be considered in any technology decision. This view avoids downtime no matter what the cause, minimizes downtime when it cannot be avoided, and works toward establishing an end-to-end, high availability (HA) infrastructure.

Readers should come away from this paper with an easy list of criteria that lets them effectively acquire, deploy and use the right BC technologies, at the right price, for any midrange or enterprise IT environment.

The Business Continuance Balancing Act

Virtually every organization would like the ability to recover all of its most recent data, almost instantly, when a disaster strikes.

In most cases, however, the reality is that most comprehensive BC technologies allowing this type of low recovery point objective (RPO) and low recovery time objective (RTO) usually come with a commensurate, high price tag that can quickly make it unaffordable to recover all data as soon as possible.

Consequently, one of the BC tradeoffs is to first identify the most business-critical applications and data, then apply a stricter set of RTO/RPO standards to these systems than to other data and systems deemed less critical. The other tradeoff may be to settle for a higher RPO or RTO with technology that fits better into the IT budget.

The end result of this effort often means the deployment of one technology solution for a critical subset of company data, while other point solutions are deployed for the data protection and longer recovery of other systems. Unfortunately, this balancing act between cost and functionality often leads to a complex patchwork of separate BC processes required to support separate applications and islands of storage.

This is not always good news for busy IT teams with little time to devote to managing such heterogeneous systems and processes.

For IT executives looking for the right BC solution to meet their needs, this is just one example of the balancing act they must perform. When evaluating BC solutions, executives must also consider other areas such as ease of implementation and on-going management, how well the technology will perform during a disaster, and whether or not they will be locked into a particular technology path or vendor once they decide on a certain solution.

Two Common BC Metrics

When defining BC and DR requirements on an application by application basis, many organizations categorize their needs based on a desired recovery time objective (RTO) and a recovery point objective (RPO):

- **Recovery Time Objective (RTO)** is the amount of time it should take to get systems back up and running after a disaster. In general, the smaller the RTO, the more costly the technology will be. The technique of immediate, synchronous replication of data to another off-site system is generally considered the most costly BC technology choice.
- **Recovery Point Objective (RPO)** should indicate how much or how little data you are prepared to lose after a disaster. If you can stand to lose the last 2 hours of e-mail data during a restore process, then the RPO for your e-mail system should be 2 hours. This would indicate that some type of backup routine needs to run every 2 hours. In general, the smaller the RPO, the more costly the technology will be.

Eight Criteria to Evaluate the Effectiveness of BC Technologies

A number of areas must be carefully weighed when evaluating the impact of potential BC solutions on existing environments. To help organizations conduct their own, careful assessment of the different BC technologies available, Dot Hill Systems has developed a holistic approach to evaluating business continuance options. This approach includes eight types of detailed evaluation criteria. These are referenced in the following table.

Business Continuance Technology Evaluation Criteria	... Explores the Following Areas of Inquiry
<p>1. Functionality</p>	<ol style="list-style-type: none"> 1. How well the solution prevents or reduces the impact of the most common business disruptions. 2. Any disk-based backup features that aid in rapid backup or restore of data. These might include areas like snapshot functionality, and the ability to identify and group application-specific data sets for faster restore. Do these features supplement existing backup processes? Are they able to replace existing methods entirely? 3. Abilities to perform synchronous and asynchronous remote replication to an off-site location. Is a separate secondary system required at the off-site location? Does the off-site equipment have to operate in standby mode only unless a disaster strikes, or can it be used for other primary production functions in the meantime? 4. The type of RTO and RPO requirements the solution can meet. 5. The technology's impact on existing infrastructure, including network bandwidth consumed, latency or CPU cycles. 6. Any preventive and reactive BC/DR activities that can be performed with the system. 7. How well the system works when deployed gradually vs. enterprise-wide. Is the system equipped to promote an end-to-end high availability infrastructure? 8. In the event of disaster, how much does the system rely on manual vs. automated processes to "fail over" to an alternate site? How complex is the failover process?
<p>2. Affordability/Cost</p>	<ol style="list-style-type: none"> 1. What are the up-front costs to implement the technology? 2. How much will the technology require in new infrastructure costs vs. its use of any existing IT resources? 3. In order to take advantage of key BC functionality, does the technology require you to buy all infrastructure components from the same vendor, or are you allowed to utilize other vendors' server, storage and network components? 4. Does the technology require the investment in more storage than you currently require? Does it offer ways to use only the storage you need and add more later without incurring significant downtime? 5. As RPO and RTO goals become smaller, how does this impact the on-going cost of the product, in terms of resources required? Will this require prioritizing critical data vs. less critical data? 6. Are there any hidden costs that might appear with on-going use of the product or the decision to deploy it on a more enterprise-wide basis? For example, are there added costs to license the system for use by more servers? 7. Are there any TCO or ROI assessments available? 8. Will the investment cost change as the technology grows to protect multiple terabytes of data?
<p>3. Visibility and Ease of Management</p>	<ol style="list-style-type: none"> 1. Does the technology help ensure uptime by offering any enterprise-wide visibility, centralized control, centralized monitoring or reporting across multiple regional offices regarding IT system performance, status of IT resources and performance against business continuance processes and IT policies? 2. If you need to operate or manage the system from another location during a disaster, how easy will that be to initiate? 3. How much effort and management time will the system require from IT staff members? 4. If a staff member moves on to another position, how hard will it be to train a new staff member?

Business Continuity Technology Evaluation Criteria	... Explores the Following Areas of Inquiry
4. Support for More Advanced or Complex Environments	<ol style="list-style-type: none"> 1. Does the technology make it easy to establish and maintain automated policies and service level agreements surrounding data protection and retention, disaster recovery, availability and restore times across the enterprise? 2. Can the business continuity services be utilized and mixed with other operating systems, other servers and storage devices, and even other data protection or replication applications from other vendors?
5. Disruptiveness Factor	<ol style="list-style-type: none"> 1. Does implementing the technology require any downtime or disruption in primary production systems? If so, how much? 2. Does implementing the technology require a wholesale upgrade in the infrastructure, or can it be implemented more gradually, in phases, as time permits? 3. Does implementing the technology require the installation and management of multiple agents to perform BC functions?
6. Adaptiveness and Flexibility	<ol style="list-style-type: none"> 1. Does implementing the technology require any downtime or disruption in primary production systems? If so, how much? 2. Does implementing the technology require a wholesale upgrade in the infrastructure, or can it be implemented more gradually, in phases, as time permits? 3. Can the technology be used to reduce or eliminate downtime or system unavailability events typically associated with extended batch jobs or complex software or system upgrades as well? 4. Can the system be easily administered from any console or server, in more than one location? 5. Does the system lock you into using a specific technology path or specific vendor-supported infrastructure? Is it open enough to allow you to take advantage of new technology developments, other vendor offerings, or changing BC priorities in your own organization? 6. Is the technology's design flexible enough to support other IT initiatives also underway, such as on-going server and storage consolidation, compliance, tiered storage or ILM, utility or grid storage, etc.?
7. Scalability	<ol style="list-style-type: none"> 1. How easy is it to expand the BC functionality to an enterprise-wide scale? 2. How will the technology choice fare in three to five years' time? Will it be able to grow to accommodate the changing needs of the organization? 3. How easy is it to apply the functionality to other sites located at a distance from the main data center?
8. Extensibility	<ol style="list-style-type: none"> 1. Can the system be used for other functions beyond its intended purpose, such as making fast, writable copies of data for use in development and testing? 2. Can the BC services be easily extended to include other data management functions, such as provisioning, data migration, logical pooling of storage resources, etc.?

Business Continuance with Dot Hill AssuredUVS™

Dot Hill Systems' holistic view of BC technologies is reflected in its own Unified Virtual Storage system AssuredUVS. The product of years of research and usage in some of the most demanding, mission-critical military and Telecom settings, the AssuredUVS's core BC technology has been built to withstand significant pressure to perform optimally and flexibly -- before, during, and after failure or disruption.

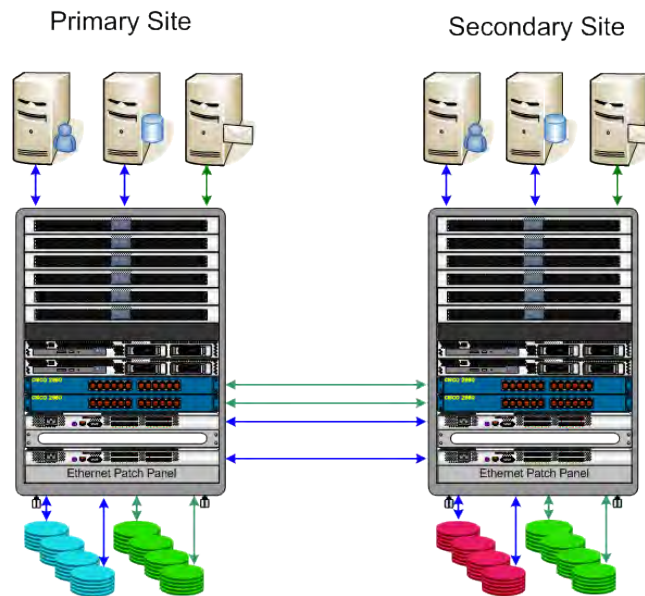


Figure 2. Business Continuance with Dot Hill AssuredUVS.

Key AssuredUVS Differentiators

Designed for use in midrange and high-end enterprise environments, Dot Hill AssuredUVS offers a completely technology and vendor-agnostic option for business continuance that is capable of providing some of the most advanced replication and failover functionality in the industry.

- Unparalleled disk-based data protection.** AssuredUVS system design includes a robust implementation of disk-based snapshot technology that is quite simply unparalleled among competitors. This technology allows IT organizations to move into disk-based data protection, in either a small or big way. Thanks to the technology's uniquely fault-tolerant design and its ability to produce snapshots that are, at once, massive, persistent and consistent, IT groups have the choice to start by using a few disk-based snapshots to supplement or replace their existing backup procedures. They can also begin on a more massive scale--pushing AssuredUVS functionality closer to a continuous data protection (CDP) model. This allows them to take efficient snapshots of only changed data as often as every few minutes -- up to the AssuredUVS's maximum allowable limit of close to 200,000 snapshots.

While allowing more rapid copying of large sets of application and file data, the true value of the AssuredUVS's snapshot technology is evidenced by the few minutes it now takes to restore critical systems and data after a disruption occurs.

In fact, the user-definable *envelope* of fall-back positions enabled by the AssuredUVS snapshot technology and supporting AssuredUVS security features can be called a snapshot-shell or "**SnapShell**". The SnapShell is an AssuredUVS guaranteed time-space field within which rapid recovery is as quick as restoring a snapshot, often literally in seconds.

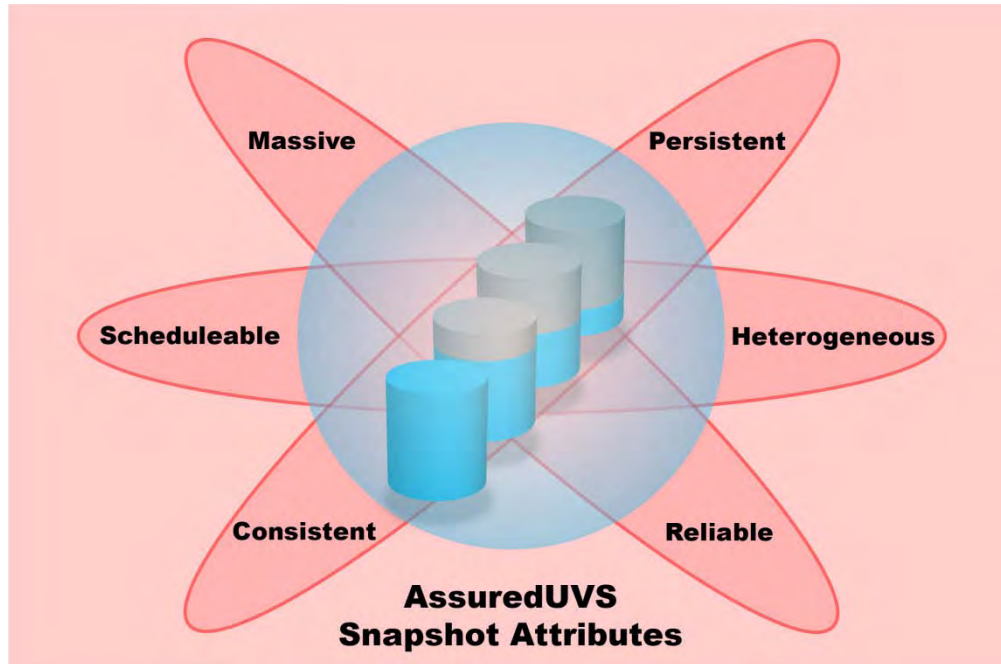


Figure 3. AssuredUVS "SnapShell" Protection Window: Up to 200,000 Snapshots

Able to generate rapid snapshots in either read-only or writeable mode (the latter of which Dot Hill calls "**virtual replicas**"), the AssuredUVS has also been used to rapidly recreate readable or writeable versions of production environments to minimize or eliminate potential downtime and slow production often associated with application or system upgrades, offline reporting and lengthy batch processing procedures. Support for development and testing environments also becomes significantly easier, with the ability to quickly create virtual replicas that can immediately be accessed by other servers and applications.

- **Business continuance--at any distance, using any storage.** For maximum business continuance coverage, the AssuredUVS is then able to combine its snapshot technology with both synchronous and asynchronous replication options--for either local or off-site replication at any distance, over Fibre Channel or IP connections. Storage resources at alternate sites operate in full active/active mode, which means no systems need stand idle and unused for production while they await occurrence of a potential disaster.

Of special interest is also the ability to be more proactive and catch potential data corruption before it can lead to a wider disruption of systems and services. Using the AssuredUVS's asynchronous, periodic replication functionality to copy recent snapshots to another location, IT organizations can schedule antivirus software to run and alert them on an on-going basis if it encounters any problems. The IT group can then isolate and correct the problem immediately and quickly restore data, if needed, from the previously known, "good state" snapshot.

- **Easy, scalable deployment options that stress flexibility and convenience.** Able to be quickly plugged into any existing SAN or NAS network of servers and storage, the AssuredUVS's own BC services are designed to be as non-disruptive as possible. They can work with existing BC or DR services in place. They can also be implemented locally, on a per application basis, based on the best possible rollout times for the IT organization. For companies wishing to deploy their BC policy across the entire organization, AssuredUVS can be immediately and easily implemented on an enterprise-wide scale, without needing to make comprehensive upgrades to the infrastructure.

- **Visibility, a unified view, and virtualized resources make it easy to monitor and optimize performance.** The system's robust virtualization functionality also allows the Dot Hill AssuredUVS system to operate as an independent, unifying layer that connects both servers and storage. In effect, the AssuredUVS brings together all heterogeneous storage resources already in the infrastructure, regardless of which vendor "box" or disk storage technology is installed. It subsequently masks the complexity of managing these systems, and presents a unified management picture of all resources where IT can quickly administer and provision new storage, gain reports about operational readiness, and apply centralized IT policies.

In masking the complexity of these physical resources, the AssuredUVS also moves any IT organization into a more logical paradigm of utility storage, storage management and business continuance by automatically consolidating and maximizing the use of available processing power and storage capacity. The end result for the IT organization and the company at large is better quality IT service delivery in several areas, including data protection, disaster recovery and business continuance. More importantly, limited IT staff will now find themselves doing less manual work, while reaping the rewards of better quality service--on a business continuance scale and beyond.

- **Pricing that is both affordable and unique.** Lastly, the AssuredUVS's pricing model is built to be affordable, and does not penalize organizations for the number servers or terabytes of data they need supported. So, there are less tradeoffs the organization needs to make when it comes to ensuring 'business as usual' in the event of disruption. It also makes it easy to scale up and grow with the system, when you need more coverage.

Conclusion

IT organizations no longer have to associate business continuance initiatives with unending, hidden costs, expensive infrastructure upgrades, complexity and frustration. There is a better way. The Dot Hill AssuredUVS story begins at the delivery of high-quality BC services at an affordable price. But, it certainly does not end there. As ESG Analyst and Founder Steve Duplessie says, "It is easier to talk about what the AssuredUVS can't do than what it can —the list is *that* extensive."³

“The AssuredUVS offers outstanding data protection features. . . Users can associate various volumes, LUNs, file systems, etc., from multiple servers into a single ‘total application consistency’ grouping – snapshot the entire group (which can span many devices) in a consistent state, and create an instantly recoverable environment. This feature alone can justify the AssuredUVS.”³

**— Steve Duplessie, Analyst and Founder
Enterprise Strategy Group**

³ Quotes in this white paper attributed to Steve Duplessie were excerpted from "AssuredUVS -- Consolidating the Storage Infrastructure," a Storage and Information Management Brief written by Steve Duplessie, and published July 25, 2005 by the Enterprise Strategy Group.