WHITE PAPER

NEVERFAIL
CONTINUOUS AVAILABILITY

BUYER'S GUIDE: CHOOSING THE RIGHT BUSINESS CONTINUITY SOLUTION

Business continuity requirements will vary according to business type and function. There is unlikely to be a "one size fits all" solution for all applications used in business.

Choosing the Right Business Continuity Solution

The new era of the customer, application availability and data protection have become mission critical requirements. The processes and tools required to protect those applications have evolved.

Today there are a myriad of technologies offering different approaches to data protection, application availability, high availability and disaster recovery. These technologies typically have at least one thing in common: they are IT-based solutions that are built to protect IT assets. When it comes to business continuity, it is imperative that choosing the right solution is a business decision based on the level of risk and disruption that can be tolerated by the different parts of the business.

For example, email is ubiquitous and preserving access to email through any type of disruption should be a priority, with 100% uptime the goal. Database applications such as sales order processing or online collaboration and content management may also require 100% uptime as the impact of downtime will be too much of a risk to the business. Other applications, such as purchase order processing, may demand no data loss, but a recovery time in the region of one hour may be acceptable. There may also be applications that are non-critical, where data can be recreated from original sources, or that are low risk and downtime measured in hours or even days is acceptable.

Business continuity requirements will vary according to business type and function. There is unlikely to be a "one size fits all" solution for all applications used in business.

Ultimately the risk to the business will be the driving factor. Assessing business need requires taking into account multiple factors. Data protection with extended recovery times may be acceptable for some functions, immediate data access for others. Protection through planned maintenance may be vital in some instances, 100% availability through disasters for others. Technology selection must address gaps between business expectations and existing IT capability. Closing the business continuity gap ensures IT delivers what business expects.

This paper explores some of the factors which will govern the selection of the right solutions to deliver an appropriate solution for business continuity.

> There are two approaches to business continuity: recovery centric or availability centric. Quite different technology is used to deliver the two approaches.

What are the options?

There are two approaches to business continuity: recovery centric or availability centric. Quite different technology is used to deliver the two approaches.

Today there are two classes of technology which can be adopted in a recovery centric strategy: backup or replication. Both are typically focused on data protection.

Ranging from legacy tape technology to continuous data protection, there are a complete set of backup technologies that will protect data. Whether held in tape format or on disk, recovering from a backup will require rebuilding databases and file systems then reconnecting with applications, which themselves may need rebuilding. Although backup technology can approach a Recovery Point Objective (RPO) of zero data loss, a Recovery Time Objective (RTO) measured in seconds will not be achievable. This is because of the focus on data protection and the separation (or lack of) application protection. Of course, backup provides great flexibility for disaster recovery as tapes can easily be protected off site, and shipped to alternative sites on demand, but recovery of the business service will likely take days.

Replication is a popular approach for availability protection. Host or storage-based replication allows exact copies of operational data to be taken. Synchronous replication provides for no data loss, but considerations such as performance, cost and bandwidth requirements for off-site protection must be taken into account. More widely spread is asynchronous replication, which has much lower operational implications and provides near zero data loss. The only loss would occur from potential transactions in flight at the time a failure occurred.

The big attraction of replication is that data recovery is not required. The online copy of data can be used immediately for failover. This is likely to require manual intervention, or significant scripting, and may require applications to be rebuilt. There is also a risk that application datasets may be missing from the replica copy if administrative processes have broken down and application upgrades have failed to be identified to administrators.

Protecting data off-site for disaster recovery also requires closer consideration. There will be bandwidth considerations, and remote systems must be available to hold an operational copy of the data.

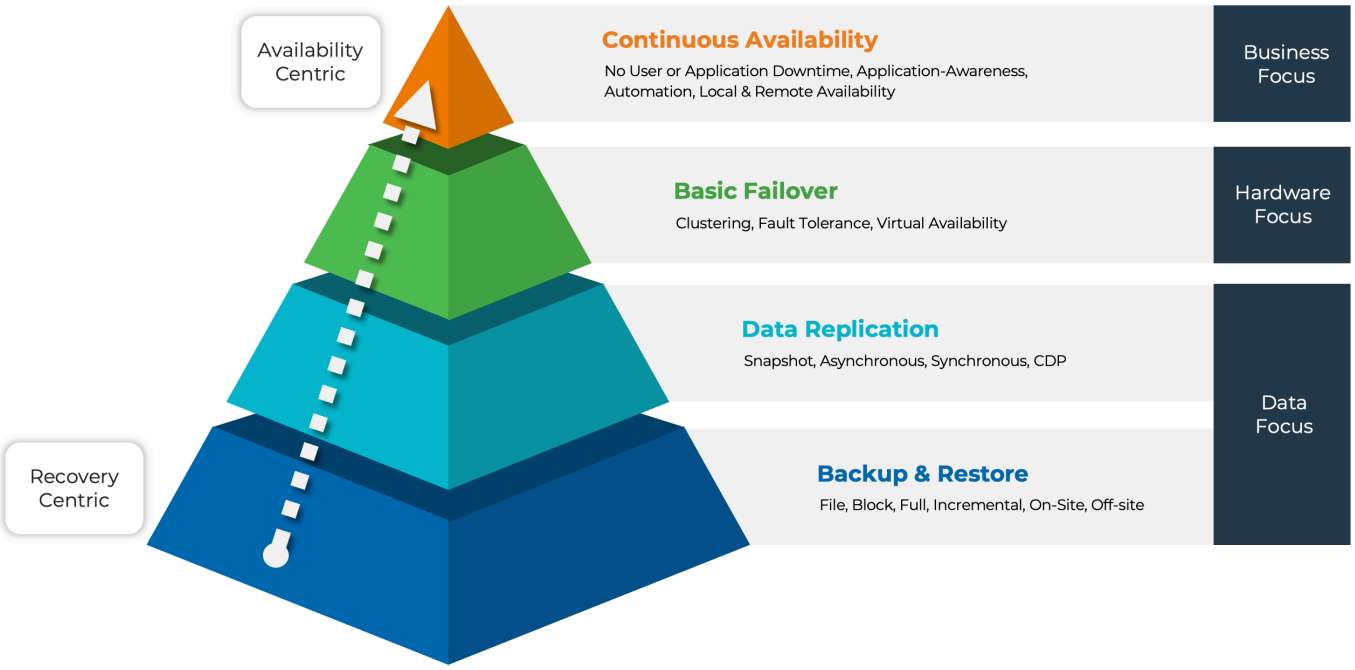

Figure 1: Availability Centric versus Recovery Centric Protection Strategies

A recovery centric strategy will, by definition, be disruptive to the business. Recovery centric approaches are applicable to less important applications as business services will stop while recovery takes place. Although the level of disruption will be reduced with a replication/failover solution, it will still not be suitable for delivering an acceptable level of availability for mission critical applications. For such applications, an application or user centric approach is required.

Historically such approaches have depended on clustering technology. Clustering allows several machines to run the same copy of the application which is accessing its data on shared storage. Clusters may consist of multiple physical and/or virtual machines and provide a platform that protects against physical or virtual machine failure. In some situations, it may also address availability for planned operations where individual machines in the cluster may be disconnected, allowing maintenance to take place.

The limitations of cluster centric approaches relate to application and processor failure. Failure situations that address the whole site, such as natural disasters, power outages and facility upgrades are not covered. Because clusters rely on shared storage and shared facilities, it is important to guard against failures at that level. In turn, this means protecting the storage from being a single point of failure. This can be costly, requiring storage virtualization and/or replication to be implemented concurrently. Additionally, virtual clusters may suffer from corruption of shared application images.

Provisioning applications across machines from the same virtual image will not guard against application corruption, and not allow application maintenance, thus limiting the level of high availability that can be delivered.

As mentioned in the introduction, there is an increasing realization that there is a disconnect between the reliance of the businesses on business critical applications and the IT approach to business continuity. The business continuity gap exists because the solutions discussed above ignore the needs of the end-user uninterrupted access to applications regardless of the cause of failure.

Results of a recent survey indicate that in regards to email, over half of organizations depend on the users to notify IT of an issue. By this time, email access has been interrupted. Addressing the needs of the user has resulted in a new discipline of high availability.

High availability solutions typically use redundancy of data and hardware, combined with data replication, in a “shared nothing” approach. While replication solutions share this approach, the difference comes when looking at the impact on the user, and hence the business. High availability solutions will provide pro-active application awareness.

Application availability will be monitored through embedded best practice facilities with a degree of self-healing provided, changes in application configuration and data dependencies will be catered for, and automation will be an option to avoid the need for manual intervention. The level of protection will embrace the end-to-end service, not

just an individual software component such as Exchange.

The choice of availability strategy will depend on many factors. Taking into account complexity in operation, total cost of ownership, skills available and the risk to the business of failure may mean combinations of the above technology are required to address business risk.

How to Assess Solutions

When looking at mechanisms to protect applications, any IT decisions need to be based on a firm foundation of business risk. It helps to look at application availability solutions in the context of four pillars of risk.

Recovery Profile

How much business disruption is acceptable? Will a backup/recovery based approach deliver against the Recovery Point and Recovery Time Objectives? The definition of Recovery Point is data based; how much data loss is acceptable?

A daily backup may lose 24 hours worth of data while a snapshot approach may lose only 15 minutes of data. Replication technology will deliver no data loss, if synchronous, or limit data loss to in-flight transactions, if asynchronous. But recovery is not limited to data. How long will it take to get the business up and running again?

Operating systems and applications will need to be rebuilt. Recovery Time Objectives should focus on minimizing or eliminating business disruption and should address data and application availability requirements.

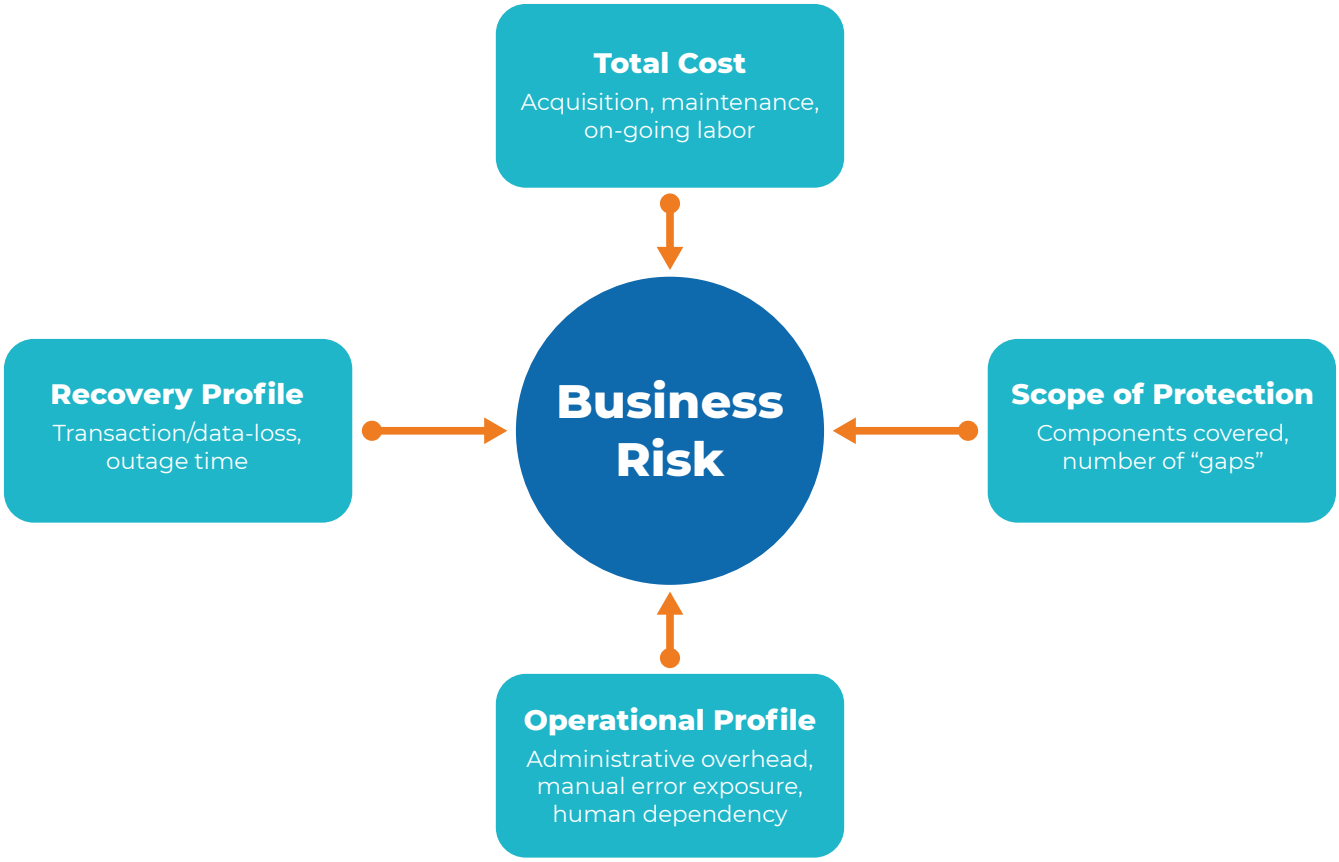

Figure 2: Availability Solution Considerations

Scope of Protection

The scope of protection directly affects the level of business disruption that can be tolerated. Limiting the scope to data backup accepts that recovery will be required, there will be data loss and there will be significant disruption to affected business services as data and applications are rebuilt. Implementing replication based solutions will eliminate disruption from loss of data, but applications will still need rebuilding and users will require reconnection. Manual intervention will be required, but the business downtime will be reduced.

Implementing cluster technology provides maximum protection against business downtime caused by server hardware failures, but site outages, data failures, application corruption and user errors will all cause significant business downtime. Outages come from network failures, processor load, data loss, application issues, human error and any number of other reasons. It's also worth remembering that protecting email is not just about protecting Microsoft® Exchange or Lotus® Domino®. Email, as a business service, needs to embrace anti-virus and anti-spam tools and mobile platforms.

Understanding the risk means understanding availability of these various components, and the gaps in protection that will bring business downtime.

Operational Capability

Not every organization has the expertise available around the clock to deal with outages at multiple levels. They may not even have the expertise and processes to ensure data is protected in the first place. Application administrators may introduce new databases or files to be protected, but unless these administrators are also responsible for high availability, will they remember to request that data protection be added? Will administration of the backup or replication regimes be updated accordingly? When failures occur and the pressure is on, are experienced personnel available to be relied upon to take the right action.

Furthermore by adding a second (failover) server into any environment, IT staff must also consider the procedural changes necessary to support the new server. Even the smallest, seemingly harmless configuration change to one server may affect the reliability of failover operations. Changes elsewhere in the IT environment (for instance to network routing tables or IP subnetting) may also have an impact on operations. Unless the availability solution is designed to account for such changes automatically, you may in fact be implementing nothing more than a false sense of security.

If user reconfiguration is required, how skilled are the users themselves? The operational capability may demand complete end-to-end automation. Only a minority of organizations do full scale disaster recovery testing because of the complexity and risk involved. Of those that are tested, it is not uncommon that the test fails, again due to complexity.

Total Cost of Ownership

The true cost of availability comes at many levels. Upfront costs are important. If existing hardware can be re-used, the ongoing cost will be reduced significantly. Solutions which replicate data asynchronously and which offer advanced data compression can also keep bandwidth costs at a minimum, dramatically impacting recurring monthly costs. The implementation costs are equally important. If significant effort is required pre-install and configure software on failover systems, make changes to DNS or Active Directory topologies, develop custom failover scripts and further customize the implementation to account for installed auxiliary applications, these will require upfront investment and on-going maintenance costs which should be factored in.

Once the solution is in place, if application configuration changes on one server need to be duplicated manually on the failover system this will incur additional personnel costs (especially if the failover system is located remotely). Where the chosen solution requires manual operation, what are the incremental costs of training and maintaining personnel on site, or at least with remote access? Ultimately, what is the true cost of downtime to the business, where cost is not just associated with lost productivity, but also with lost opportunity and reputation?

What to Look for in a Solution

Selecting an appropriate solution means considering multiple options. Ultimately, different solutions may be required for different business functions. It's important to have a clear understanding of the user and application mode of operation and the relevance in the context of availability.

The chart in Figure 3 is intended to be a quick reference for the key areas to consider before, during and after a business and technology review. This chart is not meant to be a recipe card for choosing one set of technology addressing business continuity. It may be that a backup based solution is suitable for some less critical applications whereas mission critical solutions need high availability.

In between, there may be semi-critical applications that need a replication/failover solution. In the end, the business and operational needs will drive the decision. For more information and more detail, Appendix I contains a series of bullet points which will be useful when addressing requirements and evaluating solutions.

		Backup	Replication / Failover	Clustering	High Availability	
Operational Profile	No Business Disruption	○	○	●	●	Users not impacted. No service interruption.
	No Reconfiguration	○	○	●	●	Manual changes not required. Standby system ready-to-go.
	Continuous Connectivity	○	○	●	●	No client reboot. No application restart. Users remain connected.
	Automated Operation	○	○	●	●	No manual scripting. Unattended failover and automated discovery.
	Continuous Operation	○	○	◑	●	Health checks. Resource monitoring. Fault correction and planned maintenance.
	Recovery Not Required	○	◑	○	●	Immediate failover, seamless switchback and synchronization.
Scope of Protection	Configuration	○	○	◑	●	Validation and monitoring.
	Server	○	◑	●	●	Hardware and OS monitoring. Availability protection.
	Data Protection	●	●	○	●	Replication and corruption Recovery.
	Application	○	○	◑	●	Proactive monitoring, healing and configuration end-to-end.
	Network	○	○	○	●	Access monitoring, protection, and optimization.
	Performance	○	○	◑	●	Monitoring and correction.
	Disaster	●	●	◑	●	WAN aware, local and remote secondary site support.
Recovery Profile	Recovery Point	H - D	S - M	S - M	S - M	No data loss, application and data protection.
	Recovery Time	H - D	M - H	S - M	S - M	Planned, unplanned, disaster, application and data protection. Ensure business continuity.
Total Cost	Total Cost of Ownership	$ - $$	$ - $$	$$ - $$$$$	$$- $$$	Software, hardware, implementation, management, business impact.

○	No Solution	S - M	Seconds to Minutes	$ - $$	Low to Medium Cost
◑	Partial Solution	M - H	Minutes to Hours	$$- $$$	Medium to High cost
●	Full Solution	H - D	Hours to Days	$$ - $$$$$	High to Very High Cost

Final Thoughts

Data Protection, High Availability and Disaster Recovery are all important constituents of Business Continuity. Combining the best attributes of these disciplines will make the difference between a full Business Continuity solution addressing the range of applications in use, and one with gaps in expectation and delivery.

Critical applications, ranging from email and websites to databases and mobile information platforms, are in continuous use and need to be continuously available. High availability demands that these applications are highly available, their data is continuously protected and that in the event of planned or unplanned IT outages (including disaster scenarios) they continue to operate without user disruption. Other applications may require lower levels of protection based around backup and/or failure.

One thing is clear: there is a mission critical class of application for which legacy discussions about Recovery Point and Recovery Time Objectives alone are inappropriate. Legacy approaches to availability that rely on clustering and data recovery strategies are no longer acceptable for mission critical applications.

Modern protection solutions like the Neverfail IT Continuity Engine™ (ITCE) protect mission-critical applicaitons by providing five protection levels simultaneously to ensure business is not disrupted due to planned or unplanned downtime.

1. **Server Protection** — ITCE provides availability to end user clients in the event of a hardware failure or operating system crash. When deployed, ITCE provides the ability to monitor the active/passive server pairs. If the active server fails, ITCE will cause immediate failover to the passive server. Server protection is provided for physical servers or via integration with virtual solutions such as VMware Site Recovery Manager.
2. **Application Protection** — ITCE monitors applications and services on the active server. If a protected application should fail, ITCE will restart the application or cause a graceful active/passive switchover and then restart the application on the new active server.
3. **Network Protection** — ITCE proactively monitors the ability of the active server to communicate with the rest of the network. If a problem is detected, ITCE will gracefully switch the roles of the active and passive servers allowing the previously passive server to assume an identical network identity to that of the previously active server.
4. **Performance Protection** — ITCE proactively monitors system performance attributes to ensure that protected applications are operational, performing adequately and providing service to end users. Out-of-the-box or custom modules are used to specify the attributes to monitor, the thresholds to use and the actions to take upon threshold violation.
5. **Data Protection** — ITCE ensures the data files that applications or users require in the application environment are made available should a failure occur. ITCE can be configured to protect files, folders, and even specific registry settings of the active server by mirroring them in real-time to the passive servers.

About Neverfail

Neverfail enables businesses to achieve 100% uptime through the world's most resilient business continuity and secondary storage solutions. Made for mission-critical businesses, Neverfail solutions mitigate the risk of downtime in the face of any potential outage. By delivering seamless business continuity, we empower our partners and clients to realize their full potential without the risk of downtime.

Honeywell vmware Mitel McKESSON citi Bank of America