

Enterprise Data Protection Solution Brief

Today's competitive business climate demands that information be available at all times. Protecting data, the most valuable asset of a business, is critical to the success of an organization. No company can realistically expect to lose access to information for extended periods of time without drastic business consequences. At the same time IT departments are dealing with highly complex environments where data is spread across multiple platforms and databases, in physically dispersed locations. A comprehensive data protection plan that delivers ease of management, reliability, security and scalability across all platforms, locations, applications and databases can reduce or eliminate business interruption due to data loss, while mitigating the complexity facing IT departments.

Such a plan must address all potential risks that could affect business data including:

- Hardware failures, such as data path errors, disk failures and server problems
- Application errors resulting in data corruption
- Human errors, such as accidental deletions
- Corruptions caused by viruses or failed batch jobs
- Site failures resulting from natural disasters or catastrophic events
- Change in IT infrastructure as a result of new technology introduction, business mergers
- Introduction of new projects, such as server consolidation, data migration
- Lack of or inadequately trained personnel

Data Protection Criteria

It is critical to fully assess and understand the data protection requirements of your business before designing and implementing a cost-effective data protection solution. Businesses should consider the following factors when assessing their current and future data protection requirements.

Backup Factors

As business data continues to grow, the effective backup window continues to shrink. The backup window approaches zero in mission-critical enterprise environments where it's unacceptable to have application downtime or negative system and network performance. Two key elements must be considered when performing backups:

- **Application Availability** — To perform a backup of an application, I/O operations have to be quiesced to create a valid image. It is critical to consider the amount of time for which an application can remain unavailable to its users.
- **Performance** — Creating a backup typically requires extensive data movement. This can have an adverse effect on system and network performance, impacting users of your mission-critical applications. To minimize the impact of data backup on business operations, it is important to clearly define the system and network bandwidth and performance requirements in the design of a solid data protection strategy.

Recovery Factors

Data recovery is an equally important factor in the scheme of data protection. Business transactions remain suspended until such time that data is correctly recovered and a workable environment has been restored. Two key elements that must be considered during data recovery include:

- **Data Currency/Recovery Point Objective** — The point in time to which application data must be restored following an error. It represents the amount of data loss the business is willing to tolerate.
- **Downtime Tolerance/Recovery Time Objective** — The maximum elapsed time following an error by which data must be recovered and be accessible for production use.

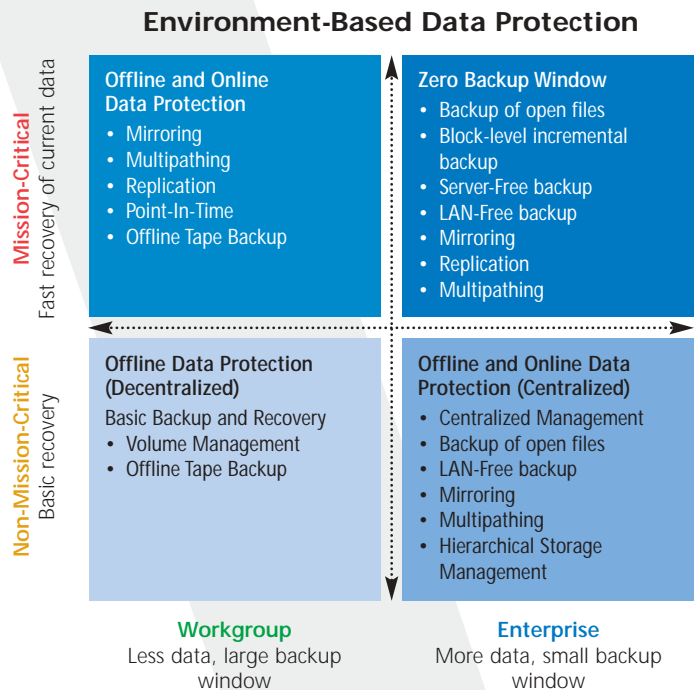
Data Protection Technologies

A comprehensive data protection plan requires a blend of technologies. Technologies that help build effective data protection solutions include:

- Redundant Array of Independent/Inexpensive Disks (RAID) offers highly available storage configurations that can withstand the failure of a physical disk device, without the loss of any data.
- Multipathing offers an alternate path to critical data in case of primary path failure.
- Point-in-Time Data Copies offer fast recovery from human error and data corruption by creating a frozen image of data on disks. This technology also offers the ability to perform offline and/or off-host tape backups while the production applications remain available to users.
- Replication technologies enable the creation of a concurrent copy of critical data at an alternate location, protecting business operations from hardware or site failures.
- Tape Backups offer data protection against a wide range of problems, including data corruptions, viruses and user errors. Tape backups deliver a fundamental level of data protection that is required for any size business. Offsite tape backups are also an essential part of many disaster recovery plans.
- Disk Backups offer an intermediate data backup and recovery point between production applications and nondisk backup medias. Disk backups and restores are fast, and often use point-in-time technology to create a complete valid image of production data. Using disk backups, data can also be destaged to nondisk media, such as tape, to offer an additional level of data protection.
- Automatic System Restores offer simplification and streamlining of server recovery process, making it unnecessary to manually reinstall operating systems or configure hardware. With a single command, a server can be completely restored in a fraction of the time.
- LAN-Free Backups offer the ability to transmit data, directly, from the server to be backed up to the backup media, making it unnecessary for backup data to utilize the LAN bandwidth. This approach results in faster backups, and also makes the LAN bandwidth more available for transmitting user requests for data.
- Server-Free Backups offer the ability to transmit data, directly between the disk device and the backup media. This approach results in extremely fast backups and off-loads the application servers from data backup processing.
- Hierarchical Storage Management (HSM) offers policy-based file migration to optimize the use of storage devices. Less-frequently accessed data can be migrated between storage devices without user knowledge or interruption in data access. HSM technology can significantly improve backup windows and recovery time objectives since less data is present in the primary medium.

Mapping Your Data Protection Needs

The type and level of data protection required for a business depends primarily on the size of the organization, the amount of data, the rate of data growth, and how business-critical the applications are.



Workgroup Environments

Workgroup-class environments generally have a viable backup window with fewer systems and relatively small amounts of data to backup. Such environments have a reasonable tolerance for downtime and can sustain the effects of some data loss. Applications in these environments can be brought offline, and cold backups of data can be performed with little or no effect on business productivity. A workgroup-class business can deploy a basic offline backup and recovery strategy. This strategy can be supplemented with RAID and dynamic multipathing to make data highly available against hardware failures in components such as disk drives, host bus adapters and cables.

Mission-Critical Workgroup Environments

The transition of a workgroup business environment into a mission-critical environment mandates the need to reduce or eliminate downtime and deliver fast recovery in case of disruptions. Backup and maintenance windows for the mission-critical operations of the business are zero or close to zero, and performance along with data currency becomes important. Mission-critical applications require online backups of open files, and demand a higher level of data protection against unforeseeable disruptive events. Technologies, such as mirroring, point-in-time data copy with fast resynchronization capabilities, and replication in conjunction with tape backups, deliver effective and efficient data protection solutions for this environment.

Enterprise Environments

Enterprise environments have large amounts of data spread across a number of systems and sites, making effective backup windows small and requiring centralized online backups and restores. System performance becomes important, as there are multiple applications competing for the same resources. Sharing of these valuable resources for nonproduction tasks, such as backups and restores, penalizes production performance. Deploying technologies that effectively use system resources can greatly reduce the overall cost outlay for an enterprise. Combining technologies like global data management, replication, mirroring, point-in-time data copy, LAN-free backups, and hierarchical storage management, can create the right enterprise-class data protection solution.

Mission-Critical Enterprise Environments

Mission-critical enterprise environments have the most stringent data availability, performance and protection requirements. These environments have zero tolerance for downtime and data loss. Offline backup and restore windows are nonexistent making online, virtual backups and restores the only feasible data protection solution. Technologies that offer extremely quick and simple recovery, such as bare metal restore, nonintrusive data protection like LAN-free and server-free backups, off-host backups and vaulting, logical volume split and join, and online replication are best-suited for mission-critical enterprise environments. These technologies coupled with other cutting-edge data protection technologies, like frozen image, incremental point-in-time data, hierarchical storage management, mirroring, and multipathing, offer the top-of-the-line data protection solutions.

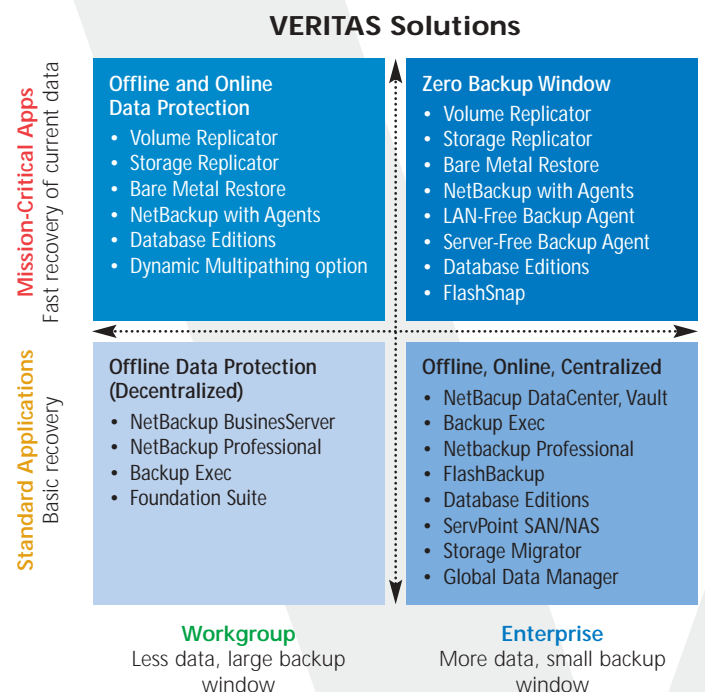
Why Choose VERITAS

VERITAS is the acknowledged leader in the data protection market, with more than 86 percent of the Fortune 500 relying on VERITAS solutions. Gartner Dataquest reports VERITAS' worldwide data protection market share increasing from 31 percent in 2000 to 40.8 percent in 2001.

- **Comprehensive Technology** — VERITAS is the only company that can provide a complete range of data protection technology from offline data protection through online data protection to the latest innovations that merge offline and online technologies.
- **Broad Platform Support** — VERITAS supports an extremely broad range of operating systems, platforms, arrays and tape libraries to ensure that you can create a consistent backup and recovery policy across your enterprise.
- **Protects the Entire Environment** — VERITAS' best-of-breed data protection technology provides support for your entire environment – from the desktop to the data center to laptops and mobile devices.

VERITAS Software Corporation
Corporate Headquarters
 350 Ellis Street
 Mountain View, CA 94043
 650-527-8000 or 866-837-4827

- **Data Protection Experts** — Customers can rely on VERITAS Consulting and VERITAS Education for the right expertise to create their data protection environment. VERITAS Consulting has the storage professionals to help assess, design, implement and manage data protection on an enterprise scale, leveraging existing resources and staff while protecting critical business data. VERITAS Education provides training on all VERITAS Software products and solutions to help reduce operating and technical infrastructure costs, increase productivity and the effectiveness of your business.
- **Flexible Support Model** — VERITAS offers a variety of technical-support models from incident and 24x7 support to fly-to-site support to meet your business needs.



For additional information about VERITAS Software, its products, or the location of an office near you, please call our corporate headquarters or visit our Web site at www.veritas.com.