CIO strategies for storage: Modernize data protection practices

Traditional approaches to data protection are no longer enough. A strategy that thoughtfully augments your legacy infrastructure with modern data protection approaches can help reduce complexity, slash costs, and minimize risk of loss—while accelerating your organization’s time to value.

The Challenge:

Traditional backup and recovery pushed to the breaking point

Ensuring your information is always available and protected is more important now than ever before with today’s 24x7x365 operations. But the traditional, “one-size-fits-all” model of weekly full backups with daily incremental data capture struggles to keep pace with the volume and change rate of data, the number and size of files and objects, and lack of off-peak production hours. These challenges can cause application availability issues, sluggish network performance, missed backup windows, unreliable and incomplete data recovery, and increased costs for backup storage.

Today, vital data is more decentralized and dispersed across multiple physical sites and device types. Remote backup to tape can be unreliable, labor intensive, and expensive to manage and secure. “Edge data” backup to a central data center can bog down or exceed available WAN bandwidth causing infrequent backup operations and compromised recovery.

In consolidated and virtualized environments, traditional backup doesn’t struggle—it breaks. The strain of virtual machine (VM) proliferation, data redundancy, excessive overhead and contention for shared resources, need for automatic discovery, application consistency, and more granular recovery increases complexity, adds cost, and potentially increases overall organizational risk.

Clearly, traditional backup and recovery has been pushed to its limits—it can’t solve today’s problems, let alone the problems of tomorrow. Additionally it’s becoming increasingly difficult to justify the cost of uncoordinated, often redundant data protection infrastructure.

The Strategy:

Modernize data protection practices

A new data and information management approach, called “modern data protection,” is key to keeping pace with today’s changing physical-virtual-cloud environments and ensuring servers, data and applications achieve always-on availability. Augmenting or even replacing traditional solutions with modern infrastructure can help you deliver flexible, cost-effective solutions for reliable protection and fast recovery.

Combining the best of traditional backup and recovery with continuity and resiliency solutions, modern data protection includes enhanced features such as compression, data deduplication, snapshots, replication and real-time backups. Additionally, modern technologies are application and virtualization aware, with built-in intelligence to optimize protection and recovery.

Modern data protection integrates with self-protecting storage. Array-based snapshots, clones, replicas and mirrors ensure data is captured as quickly and frequently as your environment needs—and is recovered just as fast. This will help you solve the challenges of too much data and not enough time, while curbing storage and management costs.

Benefits of data protection modernization

- Minimized data loss
- Maximum resource efficiency
- Streamlined and integrated workflows
- Faster, non-disruptive backups
- Rapid and flexible recovery
- Reliable, granular restores
- Hypervisor and cloud optimization
Tactical Considerations:

Choosing modern data protection solutions

While your organization will have its own set of requirements, in general you should focus on cost efficiency, simplicity, performance, scalability, and future-readiness when architecting your data protection strategy. Here is a checklist of some top features to consider, and why:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data reduction</td>
<td>Shrink backup storage requirements by 80% or more&lt;br&gt;Consolidates, compresses, and deduplicates to minimize the amount of data moved, managed, stored and protected. Minimizes backup storage requirements to reduce capital expenses, network bandwidth requirements and backup windows. Limits operational impact of backups to improve application availability. Makes it possible to backup up more frequently, increasing number of recovery points for improved service levels.</td>
</tr>
<tr>
<td>Space efficient snapshots, image-level backup</td>
<td>Achieve low-impact, near instant recovery to any RTO&lt;br&gt;Creates point-in-time copies of a full volume or set of volumes (such as hardware configuration, OS, applications and data) and stores it in a single portable file to enable rapid whole-system recovery to any physical or virtual system. Minimizes disruptions and downtime, network bottlenecks, and storage capacity. Policy-based automation quickly moves copies, reduces time and complexity associated with locating and recovering data.</td>
</tr>
<tr>
<td>Remote replication</td>
<td>Ensure business continuity during system or site outages&lt;br&gt;Creates an exact mirror copy of data on a local or remote system that can be mounted to rapidly recover from a failure. Provides minimal (asynchronous) to zero (synchronous) data loss environment for applications. Reduces time, costs, and data recovery efforts associated with traditional disaster recovery (DR) methods. Enables non-disruptive scheduled maintenance, DR testing, site workload reallocations, data center migrations and consolidations.</td>
</tr>
<tr>
<td>Continuous Data Protection (CDP)</td>
<td>Meet mission-critical high-availability requirements&lt;br&gt;Captures or tracks changes to data at a file, block or application level and immediately and automatically replicates to a secondary disk to enable recovery points from any point in time. Supports very granular recovery, ranging from crash-consistent images to logical objects such as files, mail boxes, messages and database files and logs. Eliminates protection gaps with near-zero backup windows and data loss.</td>
</tr>
<tr>
<td>Database-and application-awareness</td>
<td>Ease administration and ensure consistent recovery&lt;br&gt;Integrates with leading databases and applications, including Microsoft® SQL Server®, Microsoft Exchange Server, Microsoft SharePoint®, Oracle®, SAP®, and IBM® DB2®, to enable faster time-to-deploy, simplified management, improved application performance and availability. Provides capabilities to group all application assets, including servers, virtual machines, and databases, into a group to manage SLAs and facilitate fast, granular restores.</td>
</tr>
<tr>
<td>Virtualization-aware</td>
<td>Streamline and accelerate protection of virtual environments&lt;br&gt;Integrates with leading frameworks, such as VMware® vStorage APIs for Data Protection (VNAP), vCenter Site Recovery Management (SRM) and Microsoft® Windows Server® Volume Shadow Copy Service (VSS) to coordinate with the data protection features in the hypervisor and management layers within virtual environments. Automates discovery and management of virtual machines. Supports non-disruptive, application consistent backups and simplifies disaster recovery management and test.</td>
</tr>
<tr>
<td>Private/public cloud enabled</td>
<td>Access cloud-based resources as destination targets&lt;br&gt;Extends data protection to store backup and archive data in secure cloud-based storage tiers and cloud-based recovery sites simply and affordably. Reduces and even eliminates the need for dedicated data protection to store backup and archive data in secure cloud-based storage tiers and cloud-based recovery sites simply and affordably. Reduces and even eliminates the need for dedicated data protection. Leverages compression and deduplication to reduce network traffic and enhance WAN performance. Allows system and application recovery on cloud-based computing resources.</td>
</tr>
</tbody>
</table>

Let Dell help you choose the right path forward

Augmenting traditional data protection approaches with modern solutions, like Dell® AppAssure, Dell Quest® Software, Dell DR4000, and Dell SonicWALL®, and self-protecting storage, like Dell Compellent™, Dell EqualLogic™ and Dell PowerVault™ can help you ensure information is always available and protected—with maximum efficiency.

Learn more about Dell’s strategy for storage by visiting www.dellstorage.com/data-protection