
DATA PROTECTION MANAGEMENT: BACKING UP THE BUSINESS

Abstract

A flurry of new data regulations are arriving in the next year, and yet again businesses are expected to comply with an increased number of complex, arcane and often conflicting requirements. More than ever, companies need clear information about their data protection and data exposure. Yet data protection products are further away than ever from providing this information.

Data Protection Management: Backing Up The Business

A flurry of new data regulations are arriving in the next year, and yet again businesses are expected to comply with an increased number of complex, arcane and often conflicting requirements. In an attempt to gain compliance, business units put together data protection policies that include information about how often backups should take place, at what times of the week or month the backup can be taken, how long each backup should be kept, how quickly the data can be restored, *etc.* However, understanding if these policies are adhered to by the backup systems is another matter.

Businesses need clear information about their data protection, and conversely their data exposure, more than ever. And data protection products are further away than ever from providing this information. New technologies such as backup to disk, snapshots, replication and CDP have all proliferated in the past few years but have each found their niche and so most business today have a multitude of backup technologies. The benefit of multiple technologies is that they provide the best overall data protection policy but at the cost of visibility; it can be hard for backup administrators to be sure which technology is used to back up a given server, and attempting to expand this to a number of interlinked servers that make up an application is, as a rule, not even attempted. The result is that businesses are flying blind with respect to compliance of any data management policies that they have in place. After all, even if the backup administrators can report 99.5% success rate of their backups on a nightly basis who is to say which critical applications are affected by that 0.5% failure rate each night? Pure technical data is not enough; it must be combined with business information to provide business exposure and compliance reporting.

The problem of reconciling business and technical worlds is one that has already been tackled and is met today by asset management systems that can relate hardware and software components to business units, service criticality, cost codes, geographic locations, *etc.* The problem is that there are a plethora of these asset management systems and they each have their own interfaces. In addition, each data protection product has its own proprietary data store and so the real challenges are bringing all of this information together in a single place and providing business level reporting backed by solid technical data.

This is an area tackled by Data Protection Management (DPM) software. DPM is a discipline that can map the technical information available with backup and other data protection products to applications, business units, service criticalities, *etc.* to provide meaningful reporting for business as well as technical personnel (see Figure 1). It ensures that the information is available to the right people at the right time and in the right format, from high-level management overviews to specific business and

technical breakdowns, to ensure that the data protection environment is functioning optimally and meeting the protection policies specified by the business.

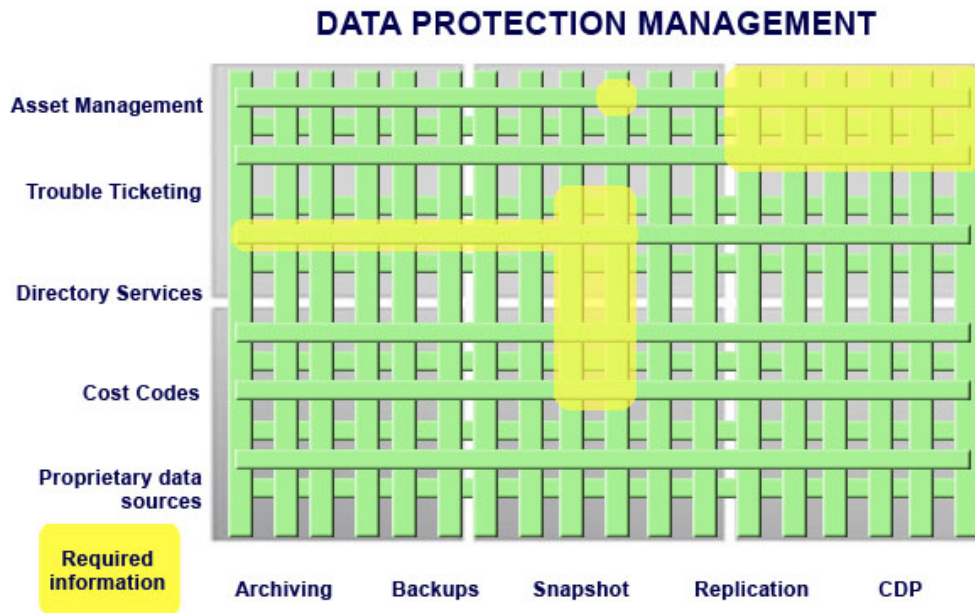


Figure 1: Graphical overview of Data Protection Management

More sophisticated DPM products have additional capabilities such as:

- real-time tie-ins to asset management and other similar databases
- historical trending to spot deviations from expected behaviour
- automated alerting of current and predicted issues
- integration with operations centres, chargeback systems and management and business portals

A full audit trail of all backups for on-demand reporting is also needed to ensure long-term compliance with regulations and the ability to respond to audit queries quickly and efficiently.

Some of the results of implementing DPM are:

- technicians are aware of the existing capacity of their backup environment and can predict future expenditure on hardware and software based on existing growth patterns
- business units have a clear picture of their data protection and data exposure to hand at any time
- management can see which business units are creating the highest workload for the backup environment and apportion costs appropriately
- the company is always able to respond to data protection audits with confidence

DPM brings advanced technical, business and management reporting to the world of data protection and gives everyone the confidence that critical data protection policies are actively enforced, ensuring that the backup environment is truly backing up the business.

WysDM is the industry's first and only data protection management (DPM) supplier to offer detailed, custom analysis of the entire data protection environment, providing the most comprehensive insight into data protection reliability, performance and compliance. Founded in 2001 by a team of storage and software executives from Goldman Sachs, Micromuse, and Storage Networks, the company has established significant traction on the customer, partner and technology fronts. Its flagship product, WysDM for Backups™, uses patent-pending Cross-Domain Correlation™ technology to analyze information collected from network, storage, system, and application domains to provide the most comprehensive, real-time backup analysis available. For more information, visit www.wysdm.com.

Copyright 2006 WysDM Software Limited. All rights reserved.

The information provided in this publication is provided "as is." WysDM Software Limited makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying and distribution of any WysDM Software products described in the publication requires an application software license.

WysDM Software and the WysDM logo are trademarks of WysDM Software Inc. All other trademarks used herein are the property of their respective owners.