

White Paper

Raising Data Protection Visibility with EMC Data Protection Advisor v6

By Jason Buffington, Senior Analyst

February 2013

This ESG White Paper was commissioned by EMC
and is distributed under license from ESG.

Contents

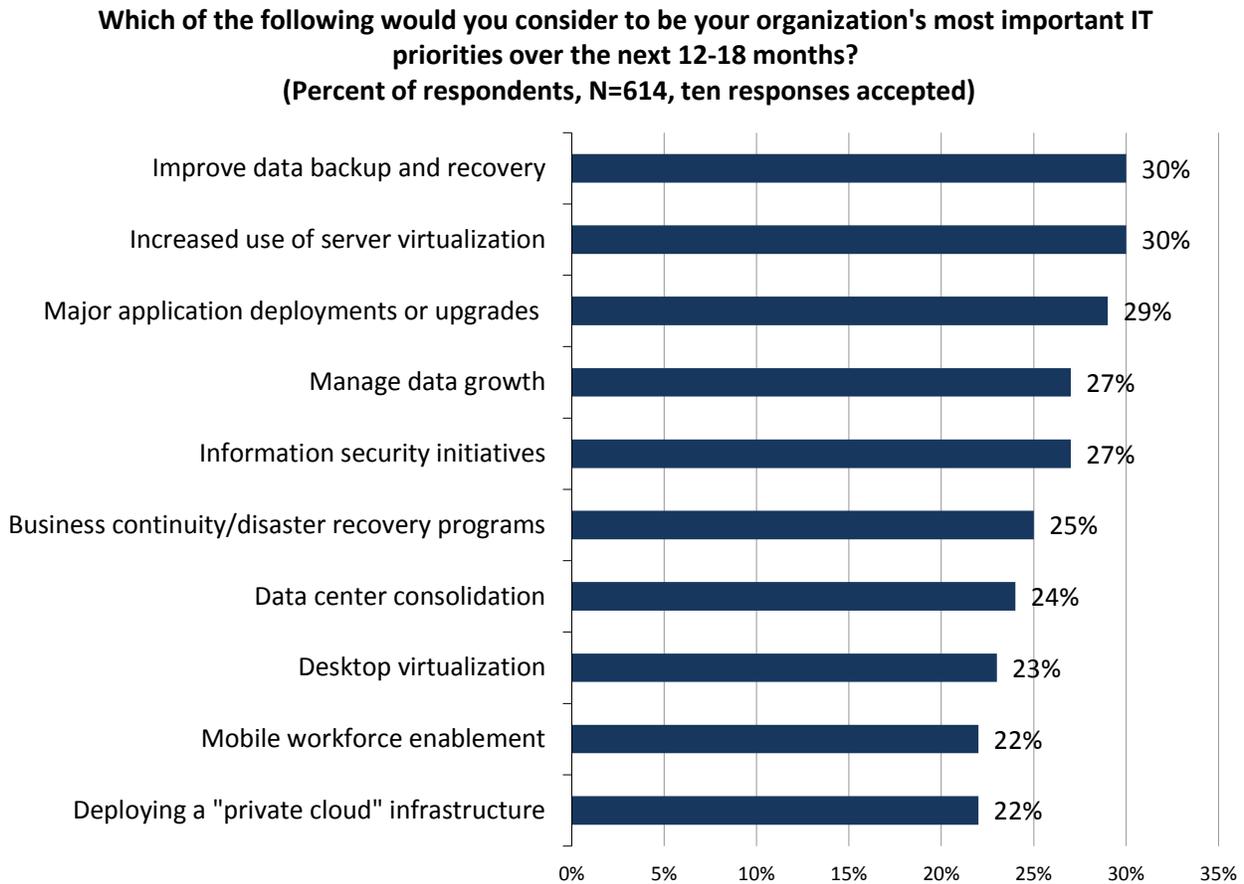
| | |
|---|----|
| Introduction | 3 |
| Backup: IT’s Arch Nemesis | 4 |
| What Makes Backup Difficult? | 4 |
| The Missing Ingredient: Data Protection Management | 4 |
| What Makes a Good DPM Solution? | 7 |
| Visibility | 7 |
| Insight | 7 |
| EMC’s Answer to Visibility and Insight: EMC Data Protection Advisor | 7 |
| EMC DPA v6 Transforms Data Protection Management..... | 8 |
| Easier Access to Information | 9 |
| Smarter and Faster Processing | 10 |
| New Capabilities | 10 |
| The Bigger Truth | 11 |

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of the Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.

Introduction

Companies of all sizes struggle to achieve data protection goals which include meeting backup and recovery windows, minimizing downtime and data loss, and ensuring recoverability of data. Issues of relentless data growth, highly-distributed data, and diminishing tolerance for downtime continue to work against IT professionals in their pursuit of minimizing risk. So, it should come as no surprise that ESG research respondents rated improving data backup and recovery as their number one IT spending priority for 2012 (see Figure 1)¹

Figure 1. Top Ten Most Important IT Priorities for 2012



Source: Enterprise Strategy Group, 2012.

Recognizing server virtualization (whose momentum will continue to advance) as the other top IT priority, combined with the fact that deploying a private cloud infrastructure is also in the top ten, shows the continued trend to deliver IT as a service, as a reliable set of capabilities that are prescribed by IT, subscribed by lines of business, consumed as needed, and paid for based on consumption. One such service is “data protection,” as the assured backup and ability-to-recover capability for many of the other IT services being offered.

But for data protection delivered as a service to be viable, regardless of private cloud (on-premises) or hybrid cloud (in conjunction with an outside service provider), one must have not just data protection tools, but monitoring and manageability of one’s data protection capabilities, current statuses, and service levels. EMC’s answer to those needs is Data Protection Advisor v6.

¹ Source: ESG Research Report, [2012 IT Spending Intentions Survey](#), January 2012.

Backup: IT's Arch Nemesis

No matter what innovations organizations launch to move their businesses forward, IT continues to battle its old nemesis: backup and recovery. Backup and recovery objectives cannot be ignored without risking great peril; organizations must be assured that data will be recoverable in the event of a problem or outage. But because they face limited resources and time to make that happen, organizations often look for solutions that make more efficient use of infrastructure, staff time, and budget—without restricting choices of applications and infrastructure. Virtualization strategies make environments more dynamic, and many backup solutions struggle to keep track of what is protected and what it not, resulting in protection gaps.

What Makes Backup Difficult?

Data growth has a tremendous impact on backup and recovery operations. Large and growing volumes of data make it hard to complete backup within the available window—and there is no margin for error, since exceeding the window results either in business interruption or unprotected data. Data growth also makes recovery slower and more complex, and can dramatically increase storage capacity requirements and associated costs.

Data protection should minimize corporate risks, such as data loss and compliance. It is a continual challenge; many organizations worry about gaps in their protection scenarios, asking:

- Is the protection we have sufficient for our needs?
- Can we restore to a recent recovery point?
- Can we track backup for all physical and virtual resources?
- Are we in compliance with the service levels that we agreed to with our stakeholders?
- Are we in compliance with the retention and recoverability mandates that we are subject to?

Another key goal is to reduce downtime during backup and recovery procedures, as the 24/7 global economy tolerates less and less business interruption. Also, compliance and audit requirements must not only be met, they must be easily verifiable to avoid fines and legal problems. The reality for today's data protection service providers (to internal stakeholders or external clients) is that green checkboxes from last night's backup jobs are not enough.

Beyond the technical challenges are the operational necessities. Of course, the *costs* of backup and recovery are always top of mind in the face of flat or shrinking budgets. Ongoing economic uncertainty is forcing organizations to keep costs down, but even in boom times, CFOs are often stingy when it comes to tasks, like backup, that don't generate revenue. Their mantra of "do more with less" is designed to improve productivity and profit, so managing the operational costs of IT tasks is key. These costs are not trivial—ESG research focused on data protection found that management costs represent 28% of the total data protection budget.²

The Missing Ingredient: Data Protection Management

Nearly all companies employ some type of backup and recovery solution—they are well acquainted not only with its objectives, but also with the dangers of neglecting it. What is missing for many is the assurance that their backups have been successfully completed and that data is recoverable. Vulnerabilities often remain because organizations are simply unaware that some of their data is inadequately protected.

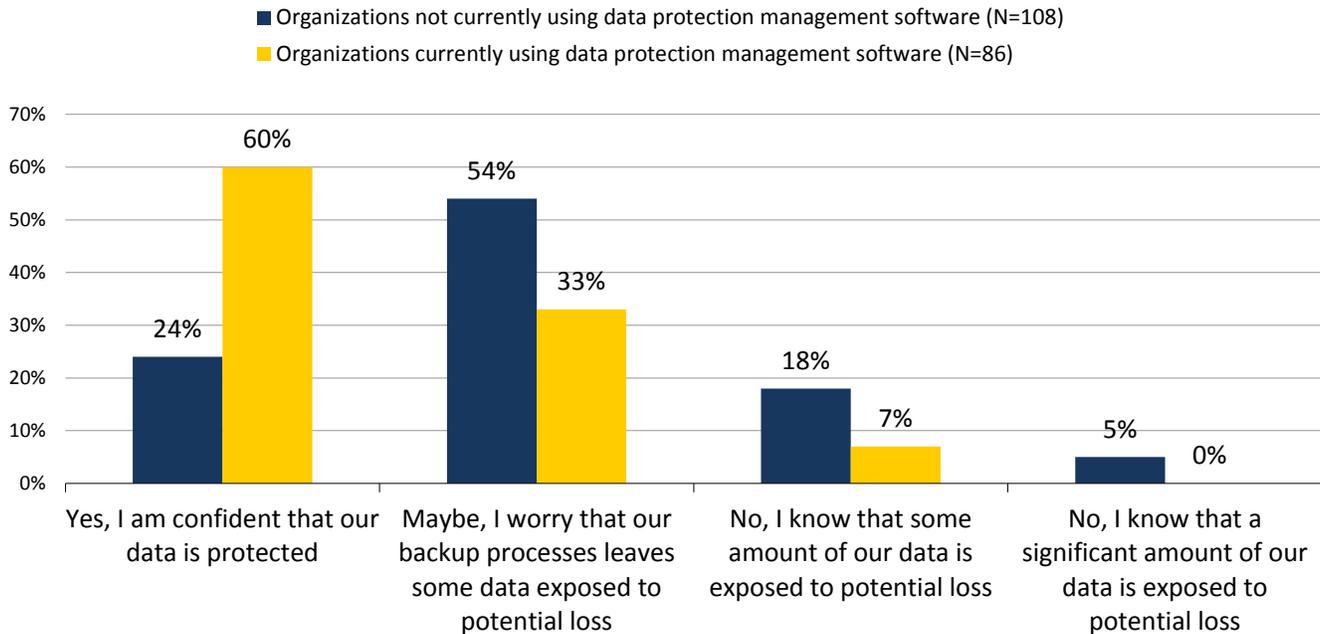
While data protection itself is job one, better data protection *management* can help organizations understand what's going on in their environment—and that's where data protection management (DPM) software comes in. ESG defines DPM as "software that performs cross-domain/multi-vendor data collections of backup, snapshot, and/or replica copy operations to deliver administrative views of data protection processes to ensure optimal data protection operations and proof that data protection processes meet compliance requirements." According to previously conducted ESG research on the topic of data protection management, less than half (44%) of survey

² Source: ESG Research Report, [2010 Data Protection Trends](#), April 2010.

respondents currently use DPM software.³ Those organizations using DPM software were more than twice as likely as those not using the technology (60% vs. 24%) to express confidence that their data protection processes provide an adequate level of protection against data loss (see Figure 2).

Figure 2. Confidence in Current Data Protection Processes, by DPM Software Usage

Confidence organizations have that current data protection processes provide an adequate level of protection against data loss, by data protection management software usage. (Percent of respondents)



Source: Enterprise Strategy Group, 2012.

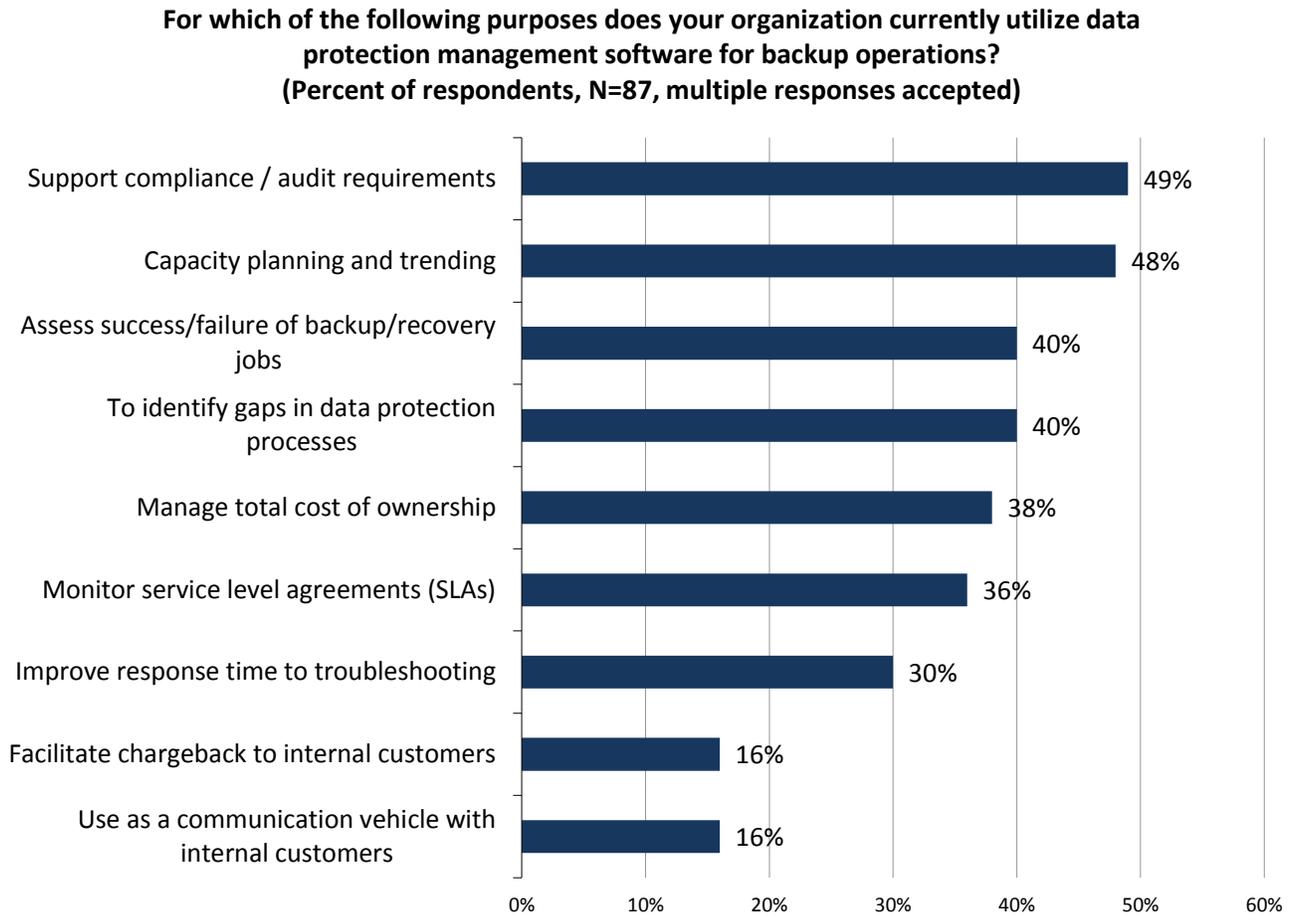
The same research also revealed a direct correlation between the amount of data being protected and the use of data protection management tools:

- 63% of organizations with more than 500TB use DPM
- 48% of organizations with 101TB to 499TB use DPM
- 47% of organizations with 26TB to 100TB use DPM
- 29% of organizations with less than 25TB use DPM

³ Source: ESG White Paper, *The Benefits of Data Protection Management Software*, March 2011.

What drives organizations to adopt DPM solutions? Given the aforementioned challenges of optimizing backup and recovery operations and mitigating risks as well as the complexity that can be assumed as data set size grows, it should come as no surprise that the top reasons ESG respondents cited for adopting DPM solutions were supporting compliance/audit requirements, capacity planning and trending, assessing the success/failure of backup/recovery jobs, and identifying gaps in data protection processes (see Figure 3).⁴

Figure 3. Reasons Organizations Use Data Protection Management Software



Source: Enterprise Strategy Group, 2012.

⁴ Ibid.

What Makes a Good DPM Solution?

While data protection itself is the critical functionality, visibility and insight into data protection status across the board can help to reduce operational expenses and improve protection confidence.

Visibility

A lack of confidence actually makes more work for IT; manually auditing backup status for different domains (physical and virtual), applications, and corporate offices is extremely time-consuming. Streamlining and automating these processes can contribute to cost savings.

Similarly, solutions that offer status information are helpful, but only if that information is easy to find. Monitoring dashboards of consolidated information as well as alerts and reports let administrators be more proactive, nipping problems in the bud instead of reacting to them.

The only way to keep the data protection environment under control is to adopt a holistic view and clearly understand what is working and what is not. For example, timely information about backup success or failure can enable IT to ensure data recoverability because what you don't know *can* hurt you. In addition, visibility into throughput and storage capacity trends can help IT administrators identify inefficiencies and bottlenecks before problems become unmanageable or impact SLAs. Moreover, IT must be able to verify and demonstrate proof of compliance to both internal customers and regulatory agencies. Solutions that offer these features save time, reduce risk, and minimize costs.

Insight

Planning for growth is rarely easy, as it requires IT to make investments based on predictions that are difficult to make when operating blindly. Administrators need visibility into actual infrastructure usage and historical trends; armed with that information, IT can identify the impacts of backup and adjust accordingly. The ability to see trends can help an organization expand just in time to protect data properly instead of over-provisioning and over-spending. In addition, tracking backup and recovery usage for chargeback can provide valuable information for planning, whether or not that information is used to actually charge users.

One good way to boost confidence in data protection is to simply do a better job at meeting SLAs and proving compliance—and that requires better information, as well as ways to communicate those good works. DPM solutions provide monitoring, alerting, and reporting to save time and provide shortcuts for troubleshooting; they also offer predictive capabilities that help IT to both identify and mitigate data protection risks, limiting surprises and avoiding future fire drills. Any solution that helps an organization provide audit reports listing data protection successes and failures, demonstrate backup and recovery SLA effectiveness, and validate that specific data sets can be successfully restored will boost confidence in the data protection paradigm.

EMC's Answer to Visibility and Insight: EMC Data Protection Advisor

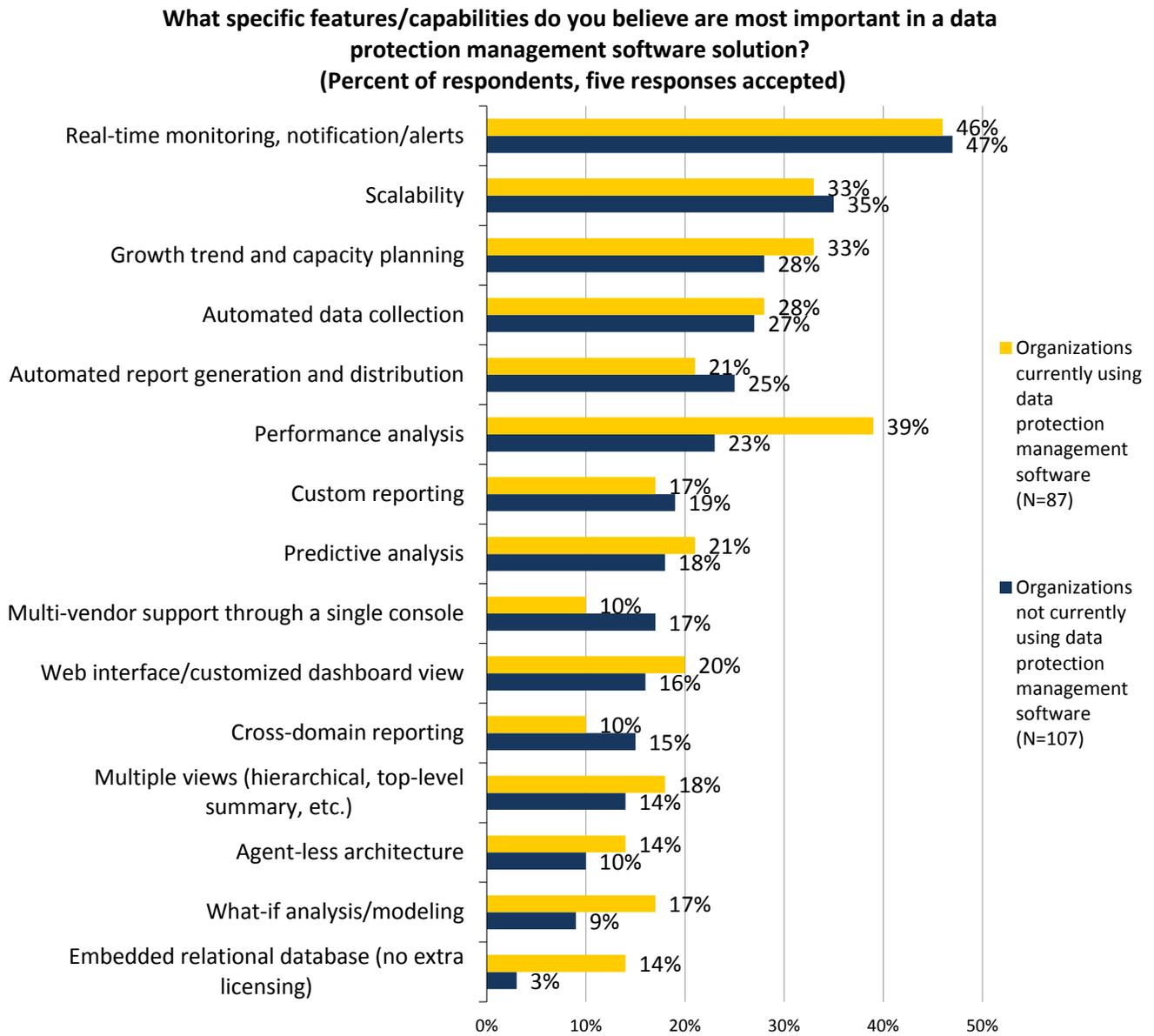
EMC Data Protection Advisor (DPA) software monitors and reports on backups, while integrating with EMC NetWorker backup software as well as EMC Avamar and Data Domain deduplication solutions (of course). But DPA's popularity stems in part from its heterogeneous nature, interfacing with many different backup solutions such as Symantec NetBackup, CommVault Simpana and IBM Tivoli Storage Manager—and providing visibility into infrastructure components such as tape libraries, tapes, deduplication storage systems, clients, servers, LAN/SAN/NAS resources, and network switches. DPA provides monitoring, alerting, troubleshooting, capacity planning, optimization, and reporting across all supported technologies and applications, enhancing insight, improving decision-making, and reducing backup and operational tasks. It also provides replication analysis to improve visibility into data replication and disaster recovery configurations to ensure compliance with service level agreements (SLAs).

EMC DPA v6 Transforms Data Protection Management

In the v6 release, EMC heralds DPA as enabling service-level monitoring of data protection by enhancing the application with a new scalable architecture along with a refreshed GUI and enhancement of the analysis engine, with the result being increased IT confidence in data protection. As a data protection service provider to internal workloads or external subscribers, the keys to success are in visibility and insight across heterogeneous data protection mechanisms. In that light, many of the features that EMC enhanced in DPA v6 align with what prospective DPM customers appear to be looking for.

Figure 4 shows how ESG research respondents ranked numerous DPM software features and capabilities—DPA v6 enhancements such as real-time monitoring and notification/alerts, scalability, and automation are high on that list. For example, DPA v6 automatically sends alerts when thresholds have been exceeded, taking a proactive approach.

Figure 4. Most Important DPM Features, by DPM Usage



Source: Enterprise Strategy Group, 2012.

Easier Access to Information

The whole purpose of DPM software is information access, so it needs to be easy to find. The redesigned user interface (UI) of DPA v6 is not only more intuitive, it follows EMC’s latest UI standards with the common EMC look and feel. As a result, customers using other EMC applications will find information in the same places and enjoy a consistent experience across different products. The benefit of maintaining navigational schemes, types of icons, and layouts across EMC software is that over-burdened IT professionals can find what they need more easily.

A key improvement is the new dashboard-driven UI (see below), which streamlines the time to value so that when you bring up the application, the information you need is already prepared and waiting for you. Administrators can customize their DPA dashboard to get relevant information at a glance without having to go find the right report, run it, and then view the results. DPA draws on prior data protection monitoring experience to present the most relevant information first (with over 700 reports available, if you need them). As an example, a “report card” can be established that automatically displays SLA details, whether or not they are being met, chargeback status, and capacity levels. With these high-level views, DPA v6 eliminates the need for a server-by-server inspection in which the user/stakeholder is forced to click into each server icon to find out its status. Instead of running a report each time the updated status is required, that information can be automatically gathered and displayed on the dashboard. Administrators can then use DPA’s granular drill-down capabilities to figure out exactly what went wrong, identify the last successful backup, and view recommended actions. DPA’s goal is to help IT administrators spend time *using* the information about their environments’ protection instead of trying to find it.

EMC Data Protection Advisor v6.0

Summary x Backup Replication + New

Alert Status by Group - Bottom 6

Scope: Business Units

| Group | Critical Alerts | Other Alerts |
|------------------------|-----------------|--------------|
| Accounting | 45 | 5 |
| Sales | 15 | 0 |
| Finance | 5 | 0 |
| Marketing | 0 | 55 |
| Research & Development | 0 | 5 |
| Public Relations | 0 | 5 |

Last Refresh: 11/9/2012 7:15am Show All 10 Groups

Backup Key Performance Indicators (KPIs)

Scope: Business Units Time Period: Last Month to Current Date

| KPI | April | May | Change | Trend |
|---------------------|--------|--------|--------|-------|
| Backup Success | 99% | 99% | - | ↔ |
| Restore Success | 87% | 85% | -2% | ↓ |
| Backups in Window | 79% | 80% | +1% | ↑ |
| Unprotected Clients | 10 | 5 | -5 | ↑ |
| Protected Data | 100 TB | 120 TB | +20 TB | |

Generated on: 11/9/2012 5:05am

Collector Health

Number of Collectors

| Collector Status | Count |
|------------------------|-------|
| Collectors Up | 75 |
| Collectors with Errors | 5 |
| Collectors Down | 2 |

Last Refresh: 11/9/2012 7:15am

Replication Key Performance Indicators (KPIs)

Scope: Business Units Time Period: Last Month to Current Date

| KPI | April | May | Change | Trend |
|----------------------|-------|-------|--------|-------|
| Objects Meeting RPOs | 99% | 99% | - | ↔ |
| Objects Meeting RTOs | 99% | 99% | - | ↔ |
| Unprotected Objects | 5 | 2 | -3 | ↑ |
| Protected Data | 50 TB | 75 TB | +25 TB | |

Generated on: 11/9/2012 5:05am

Alerts: 5 (3 New) 2 Critical (2 New) User: John Smith

Smarter and Faster Processing

Not only is the database faster, but the analysis engine has been rebuilt. With standard event processing, the system polls for certain attributes at specified intervals. EMC DPA v6 eliminates the wait time. It can correlate events across the environment in real-time, so if a problem occurs or a policy is breached, IT administrators are alerted immediately. It also provides advanced troubleshooting with more granular analysis of activities occurring in the environment. Administrators can drill down to find out exactly what is happening, get a recommendation, troubleshoot it, and resolve an issue before it becomes a bigger problem.

Not only has the DPA analysis engine been enhanced, but the access to its database has also been optimized by embedding that database to improve performance. While previous versions of DPA were efficient, they still had to reach outside of the application to leverage an external data source. With a new embedded database, DPA has broad control and immediate access to all the data, speeding up querying, dashboard displays, and report generation.

New Capabilities

While “speed, performance, and usability” were core themes of the v6 redesign, EMC also added new scenarios for data protection monitoring and virtualized environments, as well as for monitoring by service providers.

Virtualized Environments

As one might assume of VMware’s parent company, EMC continues to invest in ensuring that DPA provides the latest support for vSphere environments. Virtual machines (VMs) can be dynamically created much more easily than arbitrarily building a new physical server. This often leads to virtualized production workloads accidentally being left unprotected. The challenge is even worse as vMotion and self-service provisioned private cloud VMs become more commonplace. For example, there may be a policy to back up certain VMs, but when they are moved, reallocated, or deleted (all common occurrences), those policies can break. DPA can regularly monitor the hypervisors against the known rules and policies, and then alert the administrator as needed (such as when a data set is not backed up or a newly created VM is not covered by any policy). This way, administrators can keep a much better eye on their ever-shifting virtualized infrastructure.

Service Providers

As mentioned throughout, data protection management is about enabling the visibility and insight necessary for data protection delivered as a service, whether it is being delivered to other business units within a large company or to external clientele. With the latter, service provider model in mind, EMC enhanced the DPA architecture with scalability to support functionality for organizations of all sizes, from small companies to very large enterprises, all of whom are looking for new economic and service models for their data protection needs.

With an additional focus on service providers that utilize DPA to track data protection across their many customers, EMC has added resource partitioning to better enable monitoring a shared, multi-tenant environment. Because of these enhancements, one customer can run numerous DPA reports per day without affecting the monitoring performance of a service provider’s other customers. By fencing off resources within a DPA configuration, that one customer can have their own server while the service provider partitions out resources for other customers in real time, with no impact to other customers or downtime for anyone.

The Bigger Truth

Properly protecting data isn't enough; *knowing* that your data is properly protected (or not) is just as important.

IT environments in today's global economy are non-stop shops, with multiple critical applications, virtual servers that complicate the protection landscape, and shifting infrastructure resources. Data growth and the increased use of server virtualization continue to challenge backup plans, as IT struggles to maintain uptime and compliance while minimizing the risk of data loss. And while those challenges are tough enough for a single environment, they are even more daunting as IT teams and service providers evolve towards delivering service-based data protection to their constituents and clients. With so much going on, data protection providers have a tough task to find out exactly how each application is protected—and that can create vulnerabilities.

Data protection management solutions can help organizations maintain visibility across physical and virtual environments, but many still don't leverage them. ESG research found that DPM can make a big difference in understanding whether an organization is adequately protected or not, and what can be done to improve. DPM tools can help organizations keep track of backup success and failures, compliance policies, SLAs, and resource use.

EMC has taken its understanding of enterprise backups and has delivered Data Protection Advisor v6 to accommodate customers in need of holistic data protection monitoring across multiple backup applications and infrastructure components. In DPA v6, DPA's architecture was overhauled to improve performance and robustness, the GUI was updated and brought into alignment with other EMC software, and new dashboard views make it easier and faster to access the information IT needs. The analysis engine can now correlate events in near real time across the infrastructure; instead of waiting for polling to deliver information, alerts can be sent automatically to keep IT up to date. New capabilities were also added to support VMware virtualized infrastructures as well as broader solution provider scenarios.

The feature enhancements of DPA v6 should help EMC fulfill its goal of making data protection management "faster, easier, and smarter" by providing intuitive access to vital information concerning the protection of business applications. With better visibility and insight into a key service delivery area like backup, data protection providers can get better information with less effort—and their clients are the beneficiaries.



Enterprise Strategy Group | **Getting to the bigger truth.**