White Paper

Cloud-ready Data Protection with Dell EMC

Integrated Cloud Disaster Recovery Offers Midsized
Organizations New Options

By Christophe Bertrand, ESG Senior Analyst
and Monya Keane, Senior Research Analyst
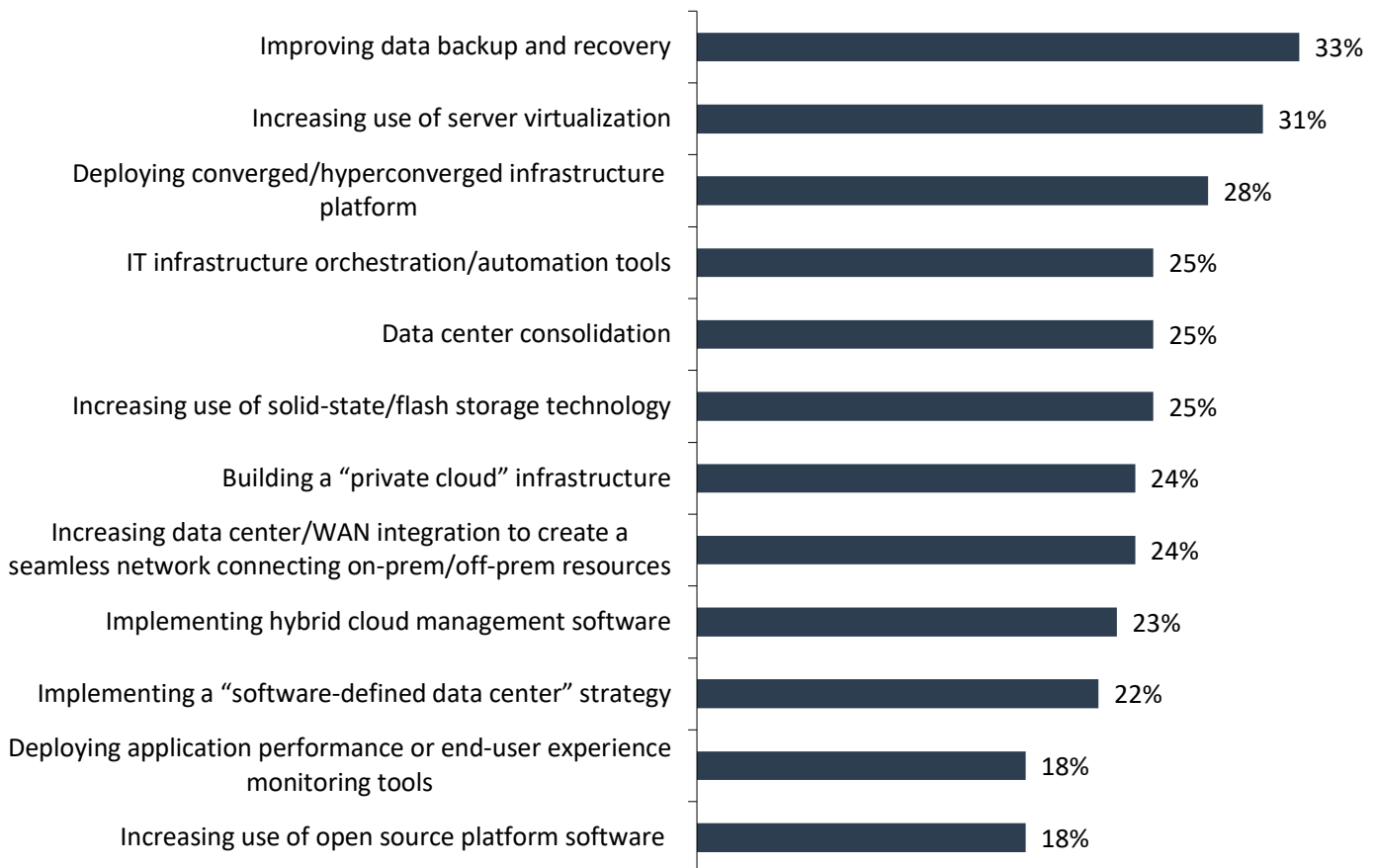August 2018

Contents

Executive Summary

When it comes to effectively and efficiently protecting growing volumes of data, midsized organizations face unique challenges. That is because they live in a world of constraints that are both operational and budgetary in nature. Cloud disaster recovery offers new options for these organizations—they can optimize their data protection economics by integrating on-premises protection solutions with cloud-based backup and recovery methods. Dell EMC's cloud-ready solutions, particularly its Integrated Data Protection Appliances with native cloud extension capabilities, along with its Data Protection Software working in conjunction with its Data Domain backup storage appliances, provide cloud disaster recovery with flexible features. These solutions enhance operational efficiency and provide midsized organizations with clear economic and operational benefits.

Introduction

Midsized organizations (defined by ESG as organizations with 100 to 2,499 employees) are vital to a modern economy. In many industries, they also are a source of innovation. Just like their larger counterparts, these organizations invest heavily in technology to run their businesses and serve their customers. Figure 1 identifies some of the critical IT modernization initiatives that midsized organizations are focusing on this year.[1]

Figure 1. 2018 Data Center Modernization Spending Priorities for Midsized Organizations

In which of the following areas of data center modernization will your organization make the most significant investments over the next 12-18 months? (Percent of respondents, N=301, five responses accepted, organizations with 100 to 2,499 employees)

Improving data backup and recovery	33%
Increasing use of server virtualization	31%
Deploying converged/hyperconverged infrastructure platform	28%
IT infrastructure orchestration/automation tools	25%
Data center consolidation	25%
Increasing use of solid-state/flash storage technology	25%
Building a "private cloud" infrastructure	24%
Increasing data center/WAN integration to create a seamless network connecting on-prem/off-prem resources	24%
Implementing hybrid cloud management software	23%
Implementing a "software-defined data center" strategy	22%
Deploying application performance or end-user experience monitoring tools	18%
Increasing use of open source platform software	18%

Source: Enterprise Strategy Group

---

[1] Source: Source: ESG Master Survey Results, *2018 IT Spending Intentions Survey*, December 2017.

Clearly, improving backup and recovery is a top data center modernization priority. This should come as no surprise, since midsized organizations are faced with stringent business pressures in an always-on digital economy with little tolerance for downtime. Data is central to business success for midsized organizations just as it is for larger organizations. It is a critical asset to protect. But midsized companies face many challenges as their data keeps growing, IT becomes more complex, and resources continue to be scarce.

When things go bad, the consequences of downtime or data loss can bring devastating business consequences to a midsized organization (see Figure 2).[2]

Figure 2. Impacts Resulting from Application Downtime or Lost Data for Midsized Organizations

Which of the following impacts to your organization could result from application downtime or lost data? Which impact is most concerning for you? (Percent of respondents, N=174, organizations with 250 to 2,499 employees)

Impact	Most concerning potential impact	All impacts that could result from downtime/lost data
Loss of customer confidence	13%	43%
Direct loss of revenue	23%	41%
Missed business opportunity	13%	40%
Loss of employee confidence	13%	40%
Damage to brand integrity	5%	30%
Diversion of resources from long-term or business critical projects	10%	29%
Subject to legal action	7%	24%
Revocation of industry or governmental accreditations	6%	18%
Reduced stock price	2%	11%
Other	1%	1%
Don't know	6%	6%

Source: Enterprise Strategy Group

Many threats to data and application availability are "equal opportunity offenders." In other words, they strike organizations of all sizes. But with fewer IT resources to draw upon, midsized organizations potentially are more vulnerable to IT incidents. They also have to deal with ongoing scarcities in certain IT skill sets, especially in the areas of cybersecurity (48%), IT architecture and planning (29%), and data protection/backup and recovery (27%).[3]

As Figure 2 showed, the potentially severe ramifications of downtime and lost data are not primarily technical in nature, but rather they are business impacts with short- and long-term consequences. And notably, impacts resulting from application downtime or lost data vary only slightly for larger organizations.

Clearly, a strong backup infrastructure that conforms to the characteristics, skill sets, and resources available to midsized organizations is needed.

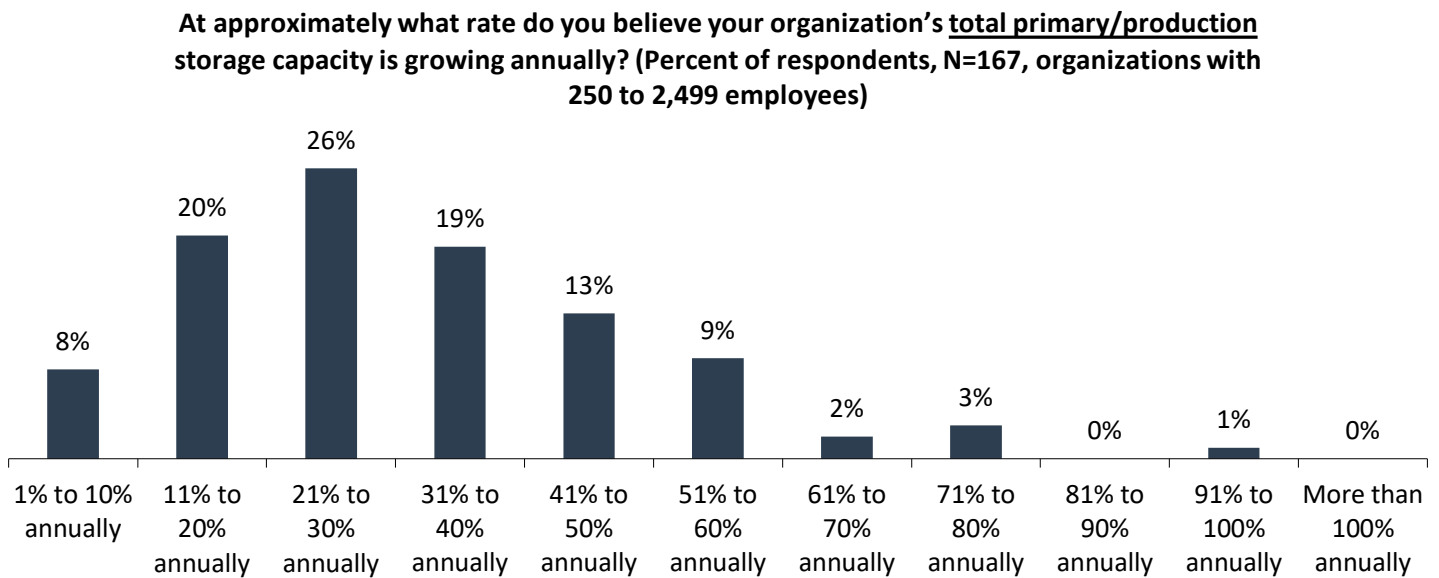[2] Source: ESG Master Survey Results, *Real-world SLAs and Availability Requirements*, May 2018.
[3] Source: ESG Master Survey Results, *2018 IT Spending Intentions Survey*, December 2017.

Data Protection in the Midmarket

As mentioned, midsized organizations face special challenges in regard to backup and recovery infrastructure, and IT complexity is one of the biggest challenges of them all. A combined 65% of respondents from midsized organizations surveyed by ESG say their IT environments have become either more or significantly more complex in the past two years, and 42% blamed the complexity on higher data volumes.[4] Another source of complexity is the need to leverage both on-premises data centers and public cloud providers; it was an issue cited by 32% of respondents from midsized organizations.

The rates of data growth at midsized organizations are dramatic—32% annually on average—meaning there is evermore data for them to manage, store, and protect (see Figure 3).[5] It is not surprising that this growth is hitting midmarket organizations to the point of being the primary driver of their IT complexity.

Figure 3. Secondary Protection Storage Required for Data Protection for Midsized Organizations

At approximately what rate do you believe your organization's total primary/production storage capacity is growing annually? (Percent of respondents, N=167, organizations with 250 to 2,499 employees)

Source: Enterprise Strategy Group

From a backup and recovery perspective, it means the IT team must build an infrastructure that can scale, allow for an optimized storage footprint, and leverage cloud-tier storage/services for off-premises recovery.

Budgets are affected by all the pressure to keep an infrastructure performing at desired business service levels. Cost considerations abound—36% of midsized organizations highlighted cost as a data protection process/technology challenge, with 24% identifying it as their top challenge.[6]

Other frequently mentioned challenges related to protecting virtual environments include reducing backup time, maintaining remote site backup and recovery, and ensuring database/application-specific backup and recovery. None of those efforts are trivial. They require deploying solutions that will provide broad, deep coverage and offer excellent recovery point objective and recovery time objective (RPO/RTO) characteristics suited for a very virtualized, very hybrid IT world.

---

[4] Source: Source: ESG Master Survey Results, *2018 IT Spending Intentions Survey*, December 2017.
[5] Source: ESG Master Survey Results, *Copy Data Management Trends*, March 2018.
[6] Source: ESG Survey, *2017 Trends in Data Protection Modernization*, December 2017.

These findings help to make clear why midsized organizations are increasingly turning to the cloud. Cloud-based data protection is a good way for a midsized company to optimize both costs and disaster recovery capabilities.

Cloud disaster recovery, also known as disaster recovery-as-a-service (DRaaS), enables IT admins to back up data and applications to a secure off-premises location that they can recover from later should the need occur. Not only do such services provide offsite protection, but they also enable virtual machines to be brought up and running in minutes (depending on the cloud vendor).

Using DRaaS is tempting. But it can also present disadvantages—for example, having different solutions for backup and recovery onsite and DR in the cloud would add complexity. DRaaS use can also mean more management consoles and support teams will be needed. And if deduplication is taking place, the IT team will need to determine if the DRaaS option provides the optimal storage cost profile.

It is also important to formally validate what RPO and RTO levels to expect, and to define what details would be involved in orchestrating a recovery process. In some cases, not having the ability to restore locally can make recoveries difficult, as can bandwidth constraints.

The hybrid on-premises-plus-cloud-hosting combination is becoming increasingly popular—more than 58% of all organizations surveyed by ESG (i.e., both midsized and enterprise organizations) use or are looking into adopting it.[7] In contrast to disaster recovery-as-a-service, hybrid IT for data protection leverages an on-premises backup solution that connects to a cloud destination such as Amazon Web Services. ESG research indicates that usage of AWS among midsized organizations has more than doubled since 2014.[8]

Additionally, ESG research shows that 45% of midsized organizations currently using IaaS are using cloud as a backup repository.[9] The benefit of this approach is that it coherently integrates the cloud into an organization's existing backup and recovery environment (which is its first line of defense onsite).

Recovery processes usually leverage virtualization and orchestration as well. Those solutions can come in the form of software, but they are also available as appliances that integrate all the needed hardware, software, and networking components. That integration typically simplifies configuration and deployment, and it reduces ongoing costs.

Dell EMC's Data Protection Portfolio: Designed for Power and Simplicity

Leveraging its many years of expertise in data protection and storage, Dell EMC introduced a protection appliance designed for midsized organizations. The new appliance, called the Dell EMC Integrated Data Protection Appliance (IDPA) DP4400, natively extends an organization's ability to protect its on-premises environment. Specifically, it combines enterprise-grade technology with simplicity and ease of use to help midsized organizations take advantage of cloud efficiencies for data protection, disaster recovery, and long-term retention.

One of the new appliance's best qualities appears to be the number of tools it offers to support initial deployment and ongoing management. The single management console and dashboard in particular would make the appliance easy for an IT generalist to use. (The powerful single management interface even includes Dell EMC Data Protection Advisor analytics.)

The IDPA DP4400 is customer deployable, requiring no expensive professional services. It comes in a 2U form factor that can grow in place from 24 TB to 96 TB with no additional hardware; it is powered by a Dell PowerEdge 14G server, and it
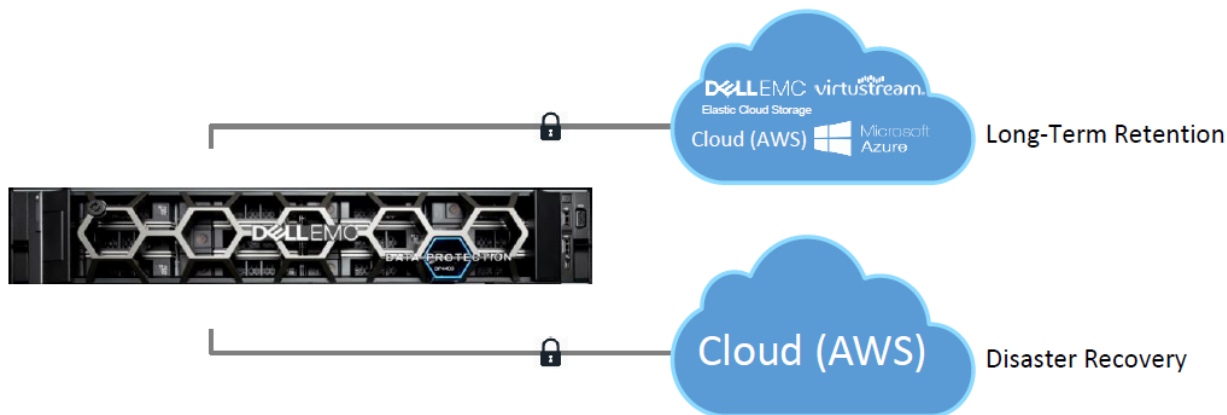
---

[7] ibid.
[8] Source: ESG Master Survey Results, *2018 IT Spending Intentions Survey*, December 2017.
[9] Source: ESG Brief, *2018 Public Cloud Infrastructure Trends*, April 2018.

leverages a layer of NVMe flash technology. Figure 4 illustrates the IDPA DP4400's cloud connections available for long-term retention and DR.

Figure 4. Dell EMC IDPA DP4400

Those native cloud-based retention capabilities happen through integration with AWS S3 and EC2. The IDPA DP4400 can store directly to S3 to optimize a midsized organization's costs—it will only use more expensive compute services in the case of a recovery process that leverages virtual machines. There is no need to purchase or deploy a separate cloud gateway. Data is compressed before sending it over to the cloud repository and change block tracking is deployed to only send new data—all to further raise performance and lower cloud storage costs.

Performing a data recovery can sometimes be a complicated exercise. The IDPA DP4400 would make that effort easier, considering there are only three clicks involved in a failover, and just two clicks needed to fail back.

The breadth of capabilities embodied within this product looks impressive, especially considering it was designed for midsized companies rather than large enterprises. For example, it comes with Dell EMC deduplication technology to provide what Dell EMC says is a 55:1 average deduplication ratio (in fact, Dell EMC guarantees "up to a 55:1 data deduplication ration" for all IDPA models). The IDPA DP4400 also integrates with VMware vSphere and a broad ecosystem of third-party applications.

The IDPA DP4400 fits the stringent data protection demands of midsized organizations through its tested set of technologies and solutions. It also provides VMware API efficiency and includes indexing for the VMware file level—that capability could offer a number of advantages from a recovery perspective.
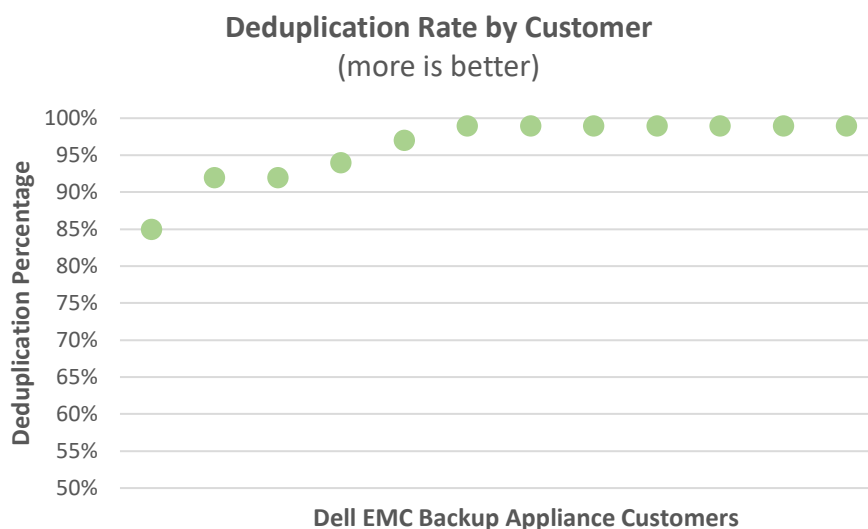
Deduplication Technology Highlights

As mentioned, data deduplication is a critical enabling technology to reduce storage capacity requirements and drive down costs. Source-side deduplication in particular generates not only capacity savings, but also backup performance improvements. With source-side deduplication, only unique data blocks are sent from the source to the target as the backup job runs, which significantly reduces network traffic. A more efficient network ultimately means backup data growth can be accommodated using existing network infrastructure.

And the less data that needs to be transferred, the faster the backup performance will be, too. Shorter backup durations allow organizations to increase the frequency of their backups. That step in turn reduces the chances that an extremely costly data-loss incident would occur (or at least, its impact would be greatly mitigated).

In June of 2018, ESG completed an economic-value assessment of the Data Domain/IDPA architectures to measure whether it would deliver the agility IT implementers need. Figure 5 shows the Data Domain/IDPA deduplication effect—namely, the percentage of deduplication achieved for each of the same 12 customer environments. Deduplication rates ranged from 85% to 99%.[10]

Figure 5. Validated Deduplication Efficiency

Deduplication Rate by Customer
(more is better)

Source: Enterprise Strategy Group

In addition, with built-in DD Boost software, Data Domain and IDPA systems support source-side *and* target-side deduplication. That support gives midsized organizations the flexibility to deploy deduplication where it makes the most sense for the environment.

Economic Efficiency

The IDPA DP4400 is the newest member of the IDPA portfolio. But Dell EMC has been designing all of its IDPA models with economic efficiency in mind. In June of 2018, ESG published the results of an economic audit of field data collected from more than 15,000 IDPA production environments.[11] ESG was able to confirm that Dell EMC IDPA hardware reduces the cost of protection by 57% to 81% versus using competitive backup software.

The Bigger Truth

With the IDPA DP4400, Dell EMC is squarely focused on helping midsized organizations. This is a very complete appliance in a 2U form factor. It comes with powerful tools and is designed with simplicity in mind for the IT generalist. While it shines in virtual environments, it is not just a point solution for VMware. It can protect many operating systems, applications, and storage systems.

The IDPA DP4400 is a solution that provides operational and economic efficiency, all grounded in the core technologies and features of the IDPA family and its software versions. It offers:

- **Storage cost optimization on-premises and in the cloud**. This is where its deduplication capabilities come into play, allowing organizations to derive significant efficiencies. This advantage is intertwined with the scalability of this

---

[10] Source: ESG White Paper, *The Economic Value of Data Domain and Integrated Data Protection Appliances (IDPA)*, June 2018.
[11] Source: ibid.

protection appliance. It can be used to reduce the number (and the cost) of systems that a midsized organization needs to deploy and manage.

- **The ability to integrate broader cloud capabilities for long-term retention and cloud disaster recovery**, leveraging the same pool of capacity-optimized protection storage for cloud backup and long-term retention.

- **A way for the organization to minimize the number of backup and recovery solutions it must use**, resulting in more IT efficiency, less risk of error, lower training costs, reduced deployment times, and simplified management.

- **Interoperability and integration between protection storage and the complex ecosystem of IT platforms**, so that application owners (e.g., database administrators and vAdmins) can utilize their own tools for supplemental protection/recovery while leveraging efficient, centralized protection storage.

- **The ability to speed deployment with integrated data protection solutions**, reducing the number of systems that need to be deployed, simplifying licensing with an all-inclusive approach, and reducing interoperability issues. The single management console and its design are also key in delivering simplicity and efficiency.

For midsized organizations that want a DIY solution or are simply not interested in a converged data protection solution, Dell EMC Data Domain 3300 combined with Dell EMC Data Protection Software delivers similar capabilities and features as the IDPA DP4400. By delivering an enterprise-class solution for midsized organizations with clear economic and operational benefits, Dell EMC is giving end-users an attractive alternative to existing offerings in the market to meet their stringent data protection service levels without breaking the bank.