

PROSYS

## Where's Your Data?

*Dell EMC's family of data protection solutions helps organizations safeguard information across physical, virtual and cloud environments.*

**W**ith so much data in so many different places, it's no wonder data protection has become so complicated in recent years. In addition to data held in on-premises servers, organizations frequently have data sitting in cloud servers and virtual servers as well as external hard drives, USB devices, PCs, laptops and smartphones. A new study conducted by the Vanson Bourne research firm concludes that 82 percent of organization do not know where their critical data is stored.

That obviously makes it difficult to be sure that backup, archive and recovery systems can actually protect, find and quickly recover all critical data. In addition to the risk of data loss or leakage, a fragmented data environment also creates regulatory concerns. For



example, the European Union's General Data Protection Regulation (GDPR) mandates that all companies with customers or employees in the EU must know exactly where every instance of someone's personal information is lo-

located. Noncompliance could result in fines of up to 4 percent of a company's global revenues.

"IT teams are finding it difficult to effectively protect data residing throughout the organization," said Michael Renner, Partner Alliance Manager, ProSys. "People are tired of buying point products from a slew of vendors and trying to make everything work together to address this situation. They are desperate for a single-source solution that protects virtual, physical and cloud workloads with high levels of automation and efficiency."

*continued on page 2*

TECH OUTLOOK

PRSRRT STD  
U.S. POSTAGE  
PAID  
Tulsa, OK  
Permit No. 2146

**“Very few companies today have all their data neatly residing in their physical data center, so that adds a lot of complexity to the data protection process. Dell EMC simplifies things with its Data Protection Suite.”**

*continued from page 1*

Dell EMC addresses this issue with its Data Protection Suite family of purpose-built software solutions that provide comprehensive protection for data and applications across all consumption models. There are five different suites, designed to deliver best-of-breed backup, recovery and archival to fit any organization’s specific needs.

**Data Protection Suite Enterprise Edition** is the most comprehensive offering. It includes all of Dell EMC’s backup and recovery products, including those for continuous replication, snapshots, traditional and deduplication backups, and archive. This suite gives organizations access to both Avamar and NetWorker backup and recovery software. Avamar features client-side deduplication for fast, daily full backups for virtual and physical environments. NetWorker is a complementary technology, delivering secure, long-term retention of backups to a variety of targeted cloud options. ProtectPoint enables direct backup from primary storage to industry-leading protection storage, eliminating performance impact on application servers. With access to all other Dell EMC data protection software, this edition allows organizations of all sizes to create a highly customized environment to protect up to 4PB of data.

**Data Protection Suite for Backup** supports many different deployment models, including deduplication backup, backup to disk, snapshot-based backup and backup to tape. It also includes both Avamar and NetWorker, and offers centralized data protection management with comprehensive reporting, monitoring, and analysis for physical and virtual environments. It is a cloud-enabled offering that allows organizations to back up data and applications within the public cloud, as well as secure long-term backup retention to targeted cloud options.

**Data Protection Suite for Applications** delivers unprecedented levels of efficiency and flexibility for mission-critical applications. It decouples backup software from the data path, allowing application owners to use native app interfaces to perform backups directly from the application server to protection storage for 20x faster backup and 10x faster recovery compared to traditional backup solutions. There is

minimal impact on application performance during backup because there is little to no data flow through the application server.

As the name suggests, **Data Protection Suite for VMware** is tailored specifically for virtualized VMware environments. As organizations virtualize more and more of their workloads, virtual machine (VM) sprawl can be an issue. New VMs are provisioned rapidly, often without data protection. With this suite, administrators can use native VMware interfaces to provision, monitor and manage the protection of their virtual workloads. It provides backup and recovery, continuous data protection for any-point-in-time recovery, backup to the cloud, monitoring and analysis, and search capabilities. It also supports virtual and physical servers along with protection of network-attached storage.

**Data Protection Suite for Archive** enables organizations to efficiently capture, index, store, manage, retrieve and dispose of both structured and unstructured data. It provides seamless access to archive content from email, file and Microsoft SharePoint. It also provides tools to accelerate search of unstructured content, increasing accuracy of discovery against deduplicated, centralized archives. These tools ultimately help companies reduce IT, operational and labor costs, as well as meet both corporate management and regulatory compliance requirements.

Organizations are shifting more and more data and applications into cloud and virtualized environments to improve their agility and flexibility, but these moves aren’t without risk. Protecting data across physical, virtual and cloud platforms can be a difficult proposition, particularly when using multiple point solutions that don’t integrate well.

“Very few companies today have all their data neatly residing in their physical data center, so that adds a lot of complexity to the data protection process,” said Renner. “Dell EMC simplifies things with its Data Protection Suite. Organizations of all sizes can get a single-source solution for ensuring the protection of files, applications and databases across all environments.”

## News Briefs

### Most Companies Support Remote Work

A new study finds that a majority of companies embrace remote work, but more than half do not have a formal remote work policy in place. For its annual Future Workforce Report, the freelancing website Upwork surveyed more than 1,000 U.S. managers. While 63 percent said they currently support a remote workforce, 57 percent lack a remote work policy.

Meanwhile, the companies with formal work-from-home policies say they have become more lenient and inclusive in the past five years. More than half (52 percent) reported that their more-relaxed policies have made it easier to find the talent they need.

Additionally, hiring managers said remote work has become more commonplace in recent years, and they predict that 38 percent of their full-time, permanent employees will work predominantly remotely within the next 10 years.

"To gain an advantage in this increasingly competitive talent climate, companies must think outside their offices or city limits and embrace a flexible, remote workforce," said Stephane Kasriel, CEO of Upwork. "Companies that refuse to support a remote workforce risk losing their best people and turning away tomorrow's top talent."

### Feds Implement DMARC to Safeguard Email

One-quarter of all email claiming to be from federal agencies is either fraudulent or otherwise unauthenticated, according to a recent survey from the cybersecurity company Agari. The firm further noted that among the 400 government domains it protects, cybercriminals targeted 90 percent of them with deceptive emails that appear to come from a federal agency.

In recognition of this threat, the U.S. Department of Homeland Security (DHS) has ordered all federal agencies to adopt an email-validation system designed to detect and prevent email spoofing. The DMARC (Domain Message Authentication Reporting and Conformance) system is specifically designed to identify spoofed email messages and notify email servers to delete those messages upon receipt — thus keeping them out of inboxes and preventing their propagation.

DMARC is built on top of two existing email authentication mechanisms, Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards. The unified solution enables domain owners to publish whitelists of approved senders, receive reports of senders attempting to use their domain names, and then block email from unapproved senders.

Agari research shows the effectiveness of DMARC. The firm says that federal domains protected by DMARC — including the U.S. Senate, Veterans Affairs, Health and Human Services and the U.S. Post Office — have seen attempted fraud send rates decrease to less than 2 percent.

## Tech Outlook

Copyright © 2018 CMS Special Interest Publications. All rights reserved.

### Editorial Correspondence:

10221 E. 61st Street  
Tulsa, OK 74133  
Phone (800) 726-7667  
Fax (918) 270-7134

**Change of Address:** Send corrected address label to the above address.

Some parts of this publication may be reprinted or reproduced in nonprofit or internal-use publications with advance written permission. Tech Outlook is published monthly by CMS Special Interest Publications. Printed in the U.S.A. Product names may be trademarks of their respective companies.

## ProSys locations

**Atlanta, GA**  
(Headquarters)  
Phone: 678-268-1300  
Toll-Free: 888-337-2626  
[Michelle.Clery@prosysis.com](mailto:Michelle.Clery@prosysis.com)

**Atlanta, GA**  
(Integration Center)  
Phone: 678-268-9000  
Toll Free: 888-337-2626  
[info@prosysis.com](mailto:info@prosysis.com)

**Austin, TX**  
Phone: 512-658-5847  
Toll Free: 888-337-2626  
[jwestmoreland@prosysis.com](mailto:jwestmoreland@prosysis.com)

**Birmingham/Montgomery, AL**  
Phone: 205-314-5746  
Toll-Free: 800-863-9778  
[info@prosysis.com](mailto:info@prosysis.com)

**The Carolinas**  
Toll-Free: 888-337-2626  
[John.Little@prosysis.com](mailto:John.Little@prosysis.com)

**Indianapolis, IN**  
Phone: 317-688-1283  
[Jay.Saini@prosysis.com](mailto:Jay.Saini@prosysis.com)

**Knoxville, TN**  
Phone: 865-310-8843  
Toll-Free: 800-863-9778  
[info@prosysis.com](mailto:info@prosysis.com)

**Louisville, KY**  
Phone: 502-719-2101  
Toll-Free: 800-863-9778  
[info@prosysis.com](mailto:info@prosysis.com)

**Mexico City**  
Phone: +52 (55) 3601 3755  
[info@prosysis.com](mailto:info@prosysis.com)

**Miami, FL**  
Phone: 305-256-8382  
Toll-Free: 800-891-8123  
[lspivot@prosysis.com](mailto:lspivot@prosysis.com)

**Mid-Atlantic**  
Phone: 800-634-2588 ext 2  
[info@prosysis.com](mailto:info@prosysis.com)

**Nashville, TN**  
Phone: 615-301-5200  
Toll-Free: 800-863-9778  
[info@prosysis.com](mailto:info@prosysis.com)

**New England**  
Toll Free: 800-634-2588 ext 1  
[info@prosysis.com](mailto:info@prosysis.com)

**Seattle, WA**  
Phone: 425-939-0342  
[sballantyne@prosysis.com](mailto:sballantyne@prosysis.com)

**Tampa, FL**  
Phone: 813-440-2410  
800-891-8123  
[lspivot@prosysis.com](mailto:lspivot@prosysis.com)

# ENSURING DATA INTEGRITY

## Purpose-built Data Domain storage appliances focus on protection to boost backup reliability.

**D**ata protection solutions are only as reliable as their underlying storage system. For years, that underlying storage was usually a general-purpose disk drive or tape drive optimized for speed and performance. Reliability can be dicey, however. One recent study found that only about 25 percent of organizations are able to restore all data in the event of a system crash.

“The issue is that the underlying storage usually was built with an emphasis on speed and performance, but not on data integrity and recoverability,” said Michael Renner, Partner Alliance Manager, ProSys. “For example, the most widely used storage file systems don’t read data back from disk to ensure it has been stored correctly — that would compromise performance and introduce latency into the system. If there’s a problem, you won’t know it until you try to restore those files.”

Recognizing these limitations, Dell EMC has made “protection storage” a central component of its data protection portfolio. Unlike general-purpose storage devices repurposed for backup, Dell EMC’s family of Data Domain backup appliances are purpose-built to handle the demands of modern backup, restore and disaster recovery requirements.

### Speed and Savings

Data Domain appliances such as the DD3300 for small and midsize organizations and the DD9300 and DD9800 for enterprise environments deliver scalable, cloud-ready protection storage. With high-speed, inline deduplication incorporated with solid-state storage, Dell EMC says these appliances also can improve backup speeds by up to 50 percent.



“The inline deduplication capabilities have a huge impact on the entire data protection environment,” said Renner. “One of the reasons conventional backup solutions are inefficient is that they repeatedly back up everything — duplicate files and sub-file data segments that exist across servers, desktops, laptops and offices.”

“When you combine all that with traditional daily incremental and weekly full backups, the amount of duplicate data is staggering. That leads to decreased performance and increased costs, and it makes searching for data in large environments a huge headache.”

Data Domain protection storage also delivers a host of cost benefits. Deduplication naturally drives down costs by enabling organizations to store more data on the same amount of physical disk space. Improved network efficiency also delivers savings. Dell EMC says the DD appliances help reduce network utilization by allowing organizations to consolidate all their data protection workloads onto a single system. Additionally, they enable direct backup from primary storage and from enterprise apps and databases such as



SAP, Oracle, IBM db2 and Microsoft SQL, which eliminates the impact on application servers and reduces the need for backup servers.

DD Boost software can further improve performance and reduce costs by distributing parts of the deduplication process to application clients or a backup server. With DD Boost, only unique data is moved from the server or clients to the Data Domain system. In a recent study, the Enterprise Strategy Group audited the impact of DD Boost backup job completions and found it enabled most organizations to complete backup jobs in an hour or less.

### **Recoverability is Key**

For all these benefits, the chief goal of DD protection storage is to ensure data recovery. That's why all Data Domain systems use the Data Invulnerability Architecture for end-to-end data verification, fault avoidance and containment, continuous self-healing and file system recoverability.

End-to-end verification ensures data integrity by confirming that data sent to backup storage is correct and re-

coverable. That involves reading data after it is written and comparing it to what was sent to disk in order to demonstrate that the data has not been corrupted and is reachable. Errors can be corrected with the self-healing capabilities from a RAID 6 dual-parity architecture.

Fault avoidance and containment features are meant to ensure that once data is verified, it remains correct. Unlike a traditional file system, which will often overwrite blocks when data changes, Data Domain systems only write to new blocks to guard against accidental overwrites. It further avoids errors through a combination of design simplicity and several fault containment features, which make it difficult for potential software errors to corrupt existing data.

“With these Data Domain appliances, Dell EMC has flipped the switch on storage for data protection purposes,” said Renner. “Unlike general-purpose storage systems that have been shifted from primary storage to data protection, Data Domain systems have been designed from the ground up to be the data store of last resort. They create a focus on data integrity without compromising on performance.”



# BETTER BACKUP

Integrated data protection appliances offer a turnkey alternative to increasingly complex backup solutions.

**D**ata protection is arguably the most critical function in IT, but it continues to be a frustrating and problematic process for most organizations. Industry surveys regularly find that organizations of all sizes are encountering significant backup issues related to cost, complexity and reliability.

Backup problems often stem from data protection technologies and processes that have not kept pace with ever-increasing amounts of data from a growing ecosystem of applications. Increased adoption of mobile computing, server virtualization, cloud services and the Internet of Things have only exacerbated the problem. Conventional backup and disaster recovery solutions are almost too cumbersome to handle it all.

Integrated data protection appliances (IDPAs) address the realities of the modern backup environment. By bundling hardware and software in a single box, IDPAs simplify the backup process and bring enterprise-class functionality to organizations of all sizes.

## Removing Complexity

In traditional enterprise backup environments, data from multiple sources is sent across the network simultaneously to a dedicated backup server, where it is processed, compressed,

deduplicated and then transferred to a backup device. Most organizations wind up adding to the complexity by using multiple backup and recovery tools.

“You have to manage multiple products such as backup software, backup servers, search servers and backup hardware — often from a variety of vendors,” said Michael Renner, Partner Alliance Manager, ProSys. “The setup is usually challenging because you have to deploy and manage multiple point solutions for different applications, platforms or data silos. It all adds up to a lengthy and time-consuming deployment that results in fragmented data protection environments that are complex and expensive to manage.”

Dell EMC offers a simplified solution with its IDPA family of turnkey data protection appliances. Along with storage, backup, search and analytics, these appliances integrate features such as encryption, fault detection, self-healing capabilities and industry-leading deduplication — an average 55:1 dedupe rate — for data residing both on-premises and in the cloud.

Dell EMC says the appliances can reduce data protection costs by up to 80 percent with the lowest cost to protect among competing products in its class. The company also says the flash-enabled appliances significantly accelerate time to value by delivering 90 percent faster box-to-backup than a traditional build-your-own solution, while delivering 20 per-

cent faster performance than the closest competitor. The flash-enabled capabilities make IDPA suitable for use as live storage in dev-test environments.

## A Powerful Package

IDPA enables organizations to protect a diverse ecosystem of applications quickly with a single system, consolidating workload protection and eliminating infrastructure sprawl. It can also scale to fit the diverse requirements of enterprises and eliminate the need for tape backups with the ability to protect up to 150PB of data directly to the public, private or hybrid cloud with native cloud tiering.

Comprehensive diagnostic, predictive and prescriptive analytics help organizations better manage their current environment and more efficiently plan for the future. Additionally, management is streamlined through a single user interface for typical daily operations. Through this interface, users can schedule and manage protection jobs, set up policies for long-term retention in the cloud and comply with protection SLAs.

IDPA appliances are VMware-optimized for VM instant access and restore, helping to meet stringent RPO/RTO requirements for VMware environments. They also provide integration with key business-critical applications and platforms such as MongoDB, Hadoop and MySQL for improved performance and greater levels of control by data owners.

## Faster, Better, Cheaper

IDPA is available in four different models to fit the needs of midsize and enterprise customers, starting at 34TB usable capacity at the entry level and scaling up to 1PB usable capacity at the high end. Services such as remote monitoring and auto-dispatch of parts from globally distributed service depots provide customers with additional confidence and peace of mind that their data and investment are protected and supported by enterprise-tested and proven serviceability from Dell EMC.

Although data backup is critical to any organization, the process has become troublesome for most IT departments. Rapid data growth is making it nearly impossible to complete backups within the available window using conventional solutions. The IDPA family of appliances delivers a simplified and cost-effective platform for processing, analyzing and storing the massive amounts of data that are being generated today.

“The Dell EMC appliances simplify and speed up data protection,” said Renner. “They free administrators from many routine data protection tasks while still enabling high levels of oversight and governance. This level of cohesion, transparency and automation is critical to ensuring simplicity and performance for backup and recovery in today’s environments.”



## Dell EMC IDPA

### Data Protection Without Compromise

Organizations need to efficiently and effectively protect an ever-increasing amount of data from a growing ecosystem of applications. Dell EMC Integrated Data Protection Appliance (IDPA) enables you to protect a diverse ecosystem of applications quickly with a single system, consolidating workload protection and eliminating infrastructure sprawl. IDPA combines protection storage, protection software, search, and analytics to reduce the complexity of managing multiple data silos, point solutions, and vendor relationships.

**Contact ProSys to learn more about  
improving your data protection capabilities  
with Dell EMC IDPA.**



www.prosys.com  
888-337-2626

© 2018 Dell Inc. or its subsidiaries. All Rights Reserved. DMC-01



# Data Protection EVERYWHERE

Only Dell EMC can cover all of your data protection needs in a single solution. The Dell EMC Protection Suite Family meets the needs of complex enterprise environments with multiple platforms and applications. It centralizes monitoring, analysis and reporting for even the most diverse environments. All your data is protected, including data that is on-premises, virtualized, stored in a public or hybrid cloud — even data born in the cloud. **Contact ProSys to learn more.**

PROSYS 

[www.prosysis.com](http://www.prosysis.com) | 888-337-2626