Tech Outlook

December 2017

PROSYS

Restoring Apps

Dell EMC overcomes limitations of traditional backup solutions to ensure rapid recovery of essential business applications.

It's all about the apps.

Over the past few years, IT operations have undergone an unmistakable shift from hardware to software. In today's software-defined infrastructure, management and control of the network, storage and data center infrastructure are automated by intelligent software rather than by hardware components. App availability has become a far more important indicator of efficiency than old metrics around server, router and switch performance.

End-users also have become more dependent on a growing ecosystem of mobile, cloud and legacy apps to do their jobs. Surveys find that the typical small business uses roughly 15 different applications, while that number surges to more than 500 in the average enterprise.

Organizations must rethink their data protection strategies for this software-centric computing model. Rather than focusing exclusively on backing up and restoring data, organizations must now ensure they can rapidly recover applications.

"If some sort of disaster hit your company tomorrow, you probably won't be getting calls from the president of the company and all the employees wondering when your servers and virtual machines are going to be recovered," said Ariel Valdes, Director, Solutions Architecture, ProSys. "They're going to want to know when they can get into email, CRM, accounting and their other essential business apps."

Dell EMC's Data Protection Suite for Applications addresses the techno-

continued on page 2

continued from page 1

logical and operational challenges associated with protecting application data. It is designed to meet the stringent service level objectives (SLOs) for mission-critical applications through such capabilities as copy data management and direct backup to protection storage.

Tricky Business

Data Protection Suite for Applications tackles some of the persistent limitations of traditional backup platforms. App recovery has always been a tricky process for these server-centric backup solutions because application data can reside in multiple locations, including databases, internal storage, removable storage, virtual machines and cloud environments.

DP Suite for Applications improves the speed and economics of application recovery by enabling backup directly to low-cost protection storage.

"With a traditional approach, you may have to search all of these locations to find unique data that is critical to a particular application, including transaction logs, external configuration data, user session data and more," said Valdes. "That's a time-consuming process, but you can't redeploy the application to its most recent state without that unique data."

To sidestep this issue, application owners often conduct their own backups. This often results in silos of application data isolated from the rest of the organization. In cases where two or more departments are using the same applications for different processes, there can be multiple copies of the same basic application data.

"That can be a real nightmare from a data protection standpoint," said Valdes. "Although you're talking about the same application, each department might have custom fields and custom data touchpoints, all on different backup schedules. That means the contents of these silos can differ in significant ways. If you don't know which represents the most current version, the restore process can actually overwrite current data with outdated data."

Self Service, With Limits

Data Protection Suite for Applications empowers application owners to conduct their own backups, but with so-called "guardrails" — backup administrators have full visibility into all self-service backups, and these backups all conform to SLOs and the governance requirements of IT's data protection policies. This enables organizations to reduce administrative overhead by decreasing the proliferation of uncoordinated backup copies from multiple sources.

Additionally, DP Suite for Applications eliminates time-consuming and potentially confusing data searches with non-disruptive discovery of data copies across the entire organization, giving organizations consolidated oversight of the environment.

DP Suite for Applications also improves the speed and economics of application recovery by enabling backup directly to low-cost protection storage. In a traditional backup environment, application owners conducting ad-hoc backups usually copy data to whatever disk is available. Often, this is to expensive primary storage. Dell EMC refers to this costly and inefficient structure as "accidental architecture."

The Dell EMC solution avoids this issue by decoupling the backup software from the data path, bypassing the backup server completely. Application owners can use native app interfaces to perform backups from the app server, primary storage or hypervisor directly to Dell EMC Data Domain protection storage. Little or no data flows through the application server, which means there is minimal impact on app performance during the backup process.

Minimizing Overhead

The solution leverages Changed Block Tracking, an incremental backup technology in which only unique blocks are sent directly to Data Domain, but are stored as full independent backups in native format. The result is faster and more efficient recovery by recovering from a full backup and by only pulling back the difference. In addition, application owners can instantly access their backups stored on Data Domain for simplified granular recovery. Dell EMC says this results in backups that are 20 times faster than traditional solutions and recovery that is 10 times faster.

While self-service backup is a core feature of DP Suite for Applications, that feature is only practical if there is overarching oversight by a backup administrator. The suite enables this central management with a single-pane-of-glass view into the entire infrastructure. Customizable dashboards with role-based access control allows visibility into all storage, copies, host and data paths, with automated provisioning, application governance and centralized oversight of the entire backup ecosystem to reduce risk and boost efficiency.

"Self-service backup by application owners has always been a problem in traditional backup environments because it leads to data silos, poor communication and wasted resources," said Valdes. "The beauty of the Dell EMC solution is that it doesn't try to eliminate self-service backup — it recognizes the value of the process and creates an environment that addresses all the challenges. It creates an environment where application owners can ensure rapid recovery and backup administrators can maintain oversight."

News Briefs

SMBs Face Storage Squeeze

Markets for artificial intelligence and machine learning technologies are growing rapidly as businesses of all shapes and sizes discover the operational and financial benefits of new analytics and automation applications. However, analysts note that the data-collection requirements of these technologies will have cascading effects on storage infrastructures — particularly for smaller organizations.

A new Fujitsu survey of senior finance professionals suggests that data storage requirements for small and midsized businesses (SMBs) will double over the next four years. There is widespread concern about this trend, with 76 percent of respondents saying they fear high or unpredictable data growth will lead to escalating data storage and management costs.

Issues of data availability, data protection and data security were cited as concerns. The financial decision-makers also expressed concern that the expandability limits of traditional disk and tape storage solutions would create unexpected investment requests. Other budget concerns surround the potential waste of equipment that prematurely reaches end-of-life, a high reliance on skilled IT staff and the challenges associated with maintaining these skills.

Respondents outlined three key characteristics they want to see in new storage technology — automation to reduce the cost and risk of manual processes, the ability to add capacity as demands increase, and overall system flexibility to deal with unpredictable growth.

Transformers Key to Smart Power Grid

North Carolina State University researchers say it may be possible to use existing solid-state transformers (SSTs) to create a smart power grid that not only distributes electricity from power companies to homes and business, but can also pull renewable energy from homes and businesses into the power grid.

The idea of a smart grid has been around for years, but it has been mostly conceptual. The new study indicates that it could move closer to reality in the near future through the use of SSTs.

Conventional transformers are fundamental components of existing power grid. They convert the high voltage power in power lines to lower voltage power that can be used safely in homes and businesses.

SSTs with embedded intelligence not only perform all the functions of conventional transformers but provide better control with high load-handling capacity and efficient bidirectional power flow by communicating with other SSTs in the system. In addition, SSTs can deliver DC voltages, unlike traditional transformers that deliver only AC voltages.

Tech Outlook

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

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

Austin, TX
Phone: 512-658-5847
Toll Free: 888-337-2626
jwestmoreland@prosysis.com

Birmingham/Montgomery, AL
Phone: 205-314-5746
Toll-Free: 800-863-9778
info@prosysis.com

The Carolinas
Toll-Free: 888-337-2626
John.Little@prosysis.com

Indianapolis, IN
Phone: 317-688-1283
Bill.sanders@prosysis.com

Knoxville, TN
Phone: 865-310-8843
Toll-Free: 800-863-9778
info@prosysis.com

Louisville, KY
Phone: 502-719-2101
Toll-Free: 800-863-9778
info@prosysis.com

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

Miami, FL
Phone: 305-256-8382
Toll-Free: 800-891-8123
lspivack@prosysis.com

Mid-Atlantic
Phone: 800-634-2588 ext 2
info@prosysis.com

Nashville, TN
Phone: 615-301-5200
Toll-Free: 800-863-9778
info@prosysis.com

New England
Toll Free: 800-634-2588 ext 1
info@prosysis.com

Seattle, WA
Phone: 425-939-0342
sballantyne@prosysis.com

Tampa, FL
Phone: 813-440-2410
800-891-8123
lspivack@prosysis.com

Limiting Risk

Increasing cyberattacks underscore the value of cyber insurance.

Virtually all organizations are now dependent on technology to one degree or another, which means they are at risk of cybercrime. Given the increasing frequency and sophistication of threats, it is no surprise that there is growing interest in cyber insurance.

According to the 2017 Cyber Survey from the Risk Management Society (RIMS), 83 percent of organizations now have a standalone cyber insurance policy. Of those without a standalone cyber policy, 84 percent indicated that other insurance policies include cyber liability coverage.

"At any given moment, cyberpredators can unleash a new hack to infiltrate an organization's system, steal or lock critical data, and cause significant business interruption damages," said RIMS President Nowell Seaman. "RIMS Cyber Survey shows that risk

professionals continue to invest in cyber insurance products and must work in tandem with their insurers and IT professionals to help develop innovative and adaptable solutions for the next generation of cyber threats."

SMBs Targeted

Ransomware has become especially threatening. Researchers at the University of California-San Diego recently estimated that cyber criminals have made more than $25 million over the past two years using malware that encrypts an organization's data and requires a payoff to unlock it.

On average, there were more than 4,000 ransomware attacks every day in 2016, according to figures from the Justice Department. That's a 300 percent increase over the previous year. Small to midsize businesses (SMBs) are particularly vulnerable.

That's no real surprise. Cyber crooks know SMBs don't have the security expertise or the budget of their enterprise counterparts. In fact, only 14 percent of SMBs rate their ability to mitigate cyber risk as highly effective. Too often, small businesses owners simply choose not to invest in preventive measures because they think they are too small to even be a target for ransomware. That could prove to be a seriously expensive miscalculation.

According to Osterman Research, 22 percent of SMBs that fell victim to a ransomware attack had to shut down their operations immediately. About 17 percent experienced downtime of 25 hours or more. On average, each incident cost SMBs more than $100,000 due to downtime.

Coverage Options

While cyber insurance isn't meant to supplant strong security measures, it can limit the financial damage from an incident and help organizations keep their doors open. A well-crafted policy will typically feature the following coverages:

Liability. This covers the legal fees, court judgments and other costs incurred after a cyberattack that results in financial harm to customers, partners or other third parties. This could involve the exposure of personal information or the unintentional transmission of a computer virus to another party.

Management liability. This option provides coverage for the liability risks faced individually by a company's officers, directors and key decision-makers while acting on behalf of the company.

Crisis management. This covers the cost of notifying consumers about a data breach that resulted in the release of private information, and also providing them with credit monitoring services. It could also cover the cost of retaining a public relations firm or launching an advertising campaign to rebuild a company's reputation.

Business Interruption. This covers loss of income due to an attack that causes an organization to temporarily shut down or otherwise limits its ability to conduct business.

Cyber extortion. This covers the settlement of a ransomware extortion threat.

Forensics. This covers the cost to hire computer forensics consultants to investigate the cause and scope of a breach, and to track down the source of the attack.

Data loss. This covers the loss, damage or destruction of valuable information assets.

It's also a good idea to look for an underwriter that provides threat mitigation services. This might include online training resources, best practices guidelines and risk assessments to help organizations learn how to avoid risk, along with incident response planning to help minimize the damage in the immediate aftermath of an incident.

Security threats are more complex, diverse and frequent than ever before. They require a layered defense that integrates a variety of hardware- and software-based tools, along with consistent training and education programs that reinforce the need for employee diligence. While it may not be possible to completely eliminate cybercrime, proper planning can limit the risk and a solid cyber insurance policy can minimize the financial exposure.

Embedded Communications

Communications Platform-as-a-Service is changing the way communications and collaboration services are delivered.

Remember when the phone system was a distinct piece of equipment that was managed by specialists? Those days are becoming a distant memory as more organizations adopt unified communications (UC) solutions. With UC, communication and collaboration tools are delivered via software running on commodity servers or in the cloud, and managed by the IT team.

Now, communications technology is moving even further away from its hardware-based roots with Communications Platform-as-a-Service (CPaaS). CPaaS is a cloud-based software development solution that makes it possible to embed rich communications functionality into a wide range of applications. And industry analysts are predicting that CPaaS will eventually overtake UC as the primary delivery mechanism for business communications.

The Gartner Magic Quadrant for Unified Communications, released in July, illustrates this trend. In order to be included in the Magic Quadrant, products had to have "the ability to integrate with other business and communications applications, such as collaboration software and contact centers, as well as application development environments such as CPaaS." The report notes that CPaaS is an increasingly popular option among organizations adopting UC solutions.

The rise of CPaaS builds upon Gartner's belief that UC is "intended principally to improve user productivity and enhance business processes." CPaaS creates significant business value by integrating communication services directly into applications and workflows.

A New Approach

The notion of combining phone systems with software is hardly new. For years, UC vendors have provided application programming interfaces (APIs) for integrating their platforms with customer relationship management (CRM) systems and other business applications. APIs make it possible to deliver "screen pops" of information to a customer service representative along with the incoming call, or allow outbound sales teams to automatically dial the customer's number from the CRM application. However, the application and the UC platform are still separate.

CPaaS is different in that real-time communication capabilities are seamlessly woven into the app itself. This offers a number of benefits, particularly for enhancing customer service. With CPaaS, developers can add click-to-call and click-to-message features to customer-facing apps, and video-enable e-commerce and customer service sites for a more engaging experience.

SMS text messaging capabilities make it easy to generate system alerts based upon specified thresholds and to send reminders and notices. For example, text messaging can be used to simplify password recovery, verification and reset procedures. Video conferencing and screen-sharing capabilities can be added to help desk software to facilitate troubleshooting and support.

Market Evolution

CPaaS has been around for years, but the technology really gained momentum in 2016. Most CPaaS offerings fall into one of two camps — "pure-play" solutions and services built into UC-as-a-Service (UCaaS) platforms.

The pure-play CPaaS solutions typically provide an API for adding communication services on top of an application. According to research firm Frost & Sullivan, the first generation of these "over-the-top" communication services provided only best-effort delivery. While most solutions have advanced beyond this model, organizations with large-scale requirements or specific needs should look for enterprise-class CPaaS services.

"Many of the popular CPaaS offerings on the market today utilize a transactional business model," said Frost & Sullivan Connected Work Industry Analyst Michael Brandenburg. "Many of these providers are not necessarily able to scale, in terms of both their infrastructure and business model, to truly support large enterprise customers."

UCaaS vendors typically offer more advanced capabilities. Their CPaaS solutions include a suite of development, testing and deployment tools, and are designed to ensure a high level of customer service.

As more organizations discover the value of CPaaS, startups and established vendors are evolving their solutions to address the needs of customers. The capabilities of CPaaS providers vary widely, however. Organizations looking to add CPaaS capabilities to their applications should clearly define their communications requirements to determine the type of CPaaS solution they need.

The traditional phone system is rapidly become a relic, replaced by platforms that use software to deliver communication and collaboration services. CPaaS takes that to the next level by turning voice, video, instant messaging and conferencing into code that can be embedded in any application.

DELL EMC

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 888-337-2626