Tech Outlook

August 2017

PROSYS

Storage on Demand

NetApp solutions meet storage demands with cloud-like agility and on-premises privacy.

Data storage is the Hydra of today's business IT environment. When the many-headed serpent of Greek mythology lost one of its heads, two more grew back in its place. In a similar way, adding capacity to address data growth often seems to generate a whole new set of problems.

"Continually adding storage ultimately creates more administrative headaches than it cures," said Bryan McCandless, Business Development Manager, ProSys. "What's more, the add-on strategy really paints you into a corner operationally and financially. When you have to purchase storage, you're tying up a lot of capital in equipment that might only temporarily meet your needs."

These factors have driven the growth of cloud storage, which effectively allows organizations to "rent" resources on demand. Not every cloud has a silver lining, however. In many cases, cloud storage comes with contractual obligations that restrict financial and operational flexibility.

NetApp address this with a pay-as-you-go storage strategy designed to deliver extreme adaptability. Using a combination of cloud-connected de-

continued on page 2

continued from page 1

livery models and innovative financing, NetApp makes it possible to right-size storage while aligning spending with business needs.

“NetApp has really taken an innovative approach to on-demand storage capacity,” said McCandless. “They’ve had a great combination of near-cloud and on-premises options for some time. They’ve upped their game recently with the creation of NetApp OnDemand, which is a unique offering that allows companies to apply a pay-per-use model to on-premises hardware.”

Tradeoffs in the Cloud

The pay-per-consumption model for storage makes sense for almost any organization because it creates budget flexibility. By shifting storage from a capital expense to an operating expense, organizations can get the capacity they need without purchasing equipment that may only temporarily meet their requirements.

The rise of the cloud has boosted this model, making it easy to purchase resources without owning infrastructure. Data is stored in an external provider's data center, and the provider manages and maintains all facets of the environment. Customers can usually choose from a variety of plans that allow them to scale usage up or down based on their needs. There are tradeoffs, however.

“In most cloud storage arrangements, the customer must commit to some baseline minimum level of storage,” said McCandless. “If you need more than that, you naturally pay for additional capacity. But what if you need less than your contracted baseline? Sometimes, you can actually wind up paying a penalty if you use less than was estimated at the beginning of the agreement.

“In other cases, you may not want to lock into a baseline. In an application development environment, for example, you may need to rapidly scale up or down depending on your development and testing cycles. A cloud provider can give you that flexibility but you’re going to pay a premium for it.”

Maintaining Control

Surveys show that many businesses remain concerned about data privacy in the cloud. Although it is likely that large cloud providers have stronger security policies and practices than all but the largest enterprise organizations, there’s always a chance that sensitive data could be vulnerable. For example, the recent Verizon breach exposed 14 million customer accounts when a vendor’s employee accidently allowed external access to a cloud storage area.

NetApp’s cloud-connected solutions are designed to let organizations access cloud storage resources while maintaining complete control over their data. With NetApp Private Storage (NPS) for Cloud, customers store data on their own storage systems inside a cloud-connected colocation facility, which allows the data to remain private just outside the cloud.

The NPS private cloud can be connected to hyperscale cloud providers such as AWS, Azure and Bluemix for on-demand scalability. This connection is made through the Equinix Cloud Exchange, an advanced interconnection solution that enables on-demand, direct network connectivity to multiple cloud providers. NetApp’s Cloud Sync Service engine synchronizes data transfers between local storage and the public cloud.

NetApp also offers NPS as a Service, which provides all of the benefits of NPS for Cloud but without the need for a capital expenditure. It can be deployed as a single-tenant or multitenant private cloud at an Equinix colocation facility.

NetApp OnDemand

NetApp OnDemand is a significant departure from other on-demand storage solutions. It combines the benefits of on-premises infrastructure, the flexibility of a usage-based consumption model, and the agility of the public cloud. The key differentiator is that NetApp retains ownership of equipment installed, and simply delivers the necessary storage capacity.

The OnDemand program begins with an initial “service design workshop” in which NetApp system administrators visit the customer site and advise on implementation and service levels. Using the OnCommand Insight tool, NetApp examines all workloads to determine the storage needs for each. That data will form the basis of the service level agreement.

Customers can choose to have the equipment installed on-premises or in an Equinix colocation facility for use with the NPS for Cloud solution.

“Unlike other on-demand solutions where you might wind up buying more capacity than you need, you really only pay for what you use with NetApp OnDemand,” said McCandless. “NetApp installs all the storage up front, and it is available immediately for your use.

“You use whatever capacity you need when you need it. There’s no price negotiation, no procurement process and no new contracts to approve. It’s a remarkably seamless process.”

News Briefs

New Malware Targets Industrial Systems

A December 2016 power blackout in the Ukraine capital city of Kiev was the result of a cyberattack featuring a new type of malware designed to target critical infrastructure. Researchers say this new strain can manipulate industrial control system (ICS) protocols to sabotage power grids, transportation controls, water and gas utilities, and other industrial systems.

Two different security firms have analyzed the malware. San Antonio-based Dragos calls it "CrashOverride," while Slovakia-based ESET calls it "Industroyer."

Researchers say it is capable of directly controlling electricity substation switches and circuit breakers. The potential impact may range from simply turning off power distribution, triggering a cascade of failures, to more serious damage to equipment.

The National Cybersecurity and Communications Integration Center (NCCIC) is still investigating the reports but says the malware appears to focus on organizations using ICS protocols IEC101, IEC104 and IEC61850, which are more commonly used outside the U.S. in electric power control systems.

"Industroyer's ability to persist in the system and to directly interfere with the operation of industrial hardware makes it the most dangerous malware threat to industrial control systems since the infamous Stuxnet, which successfully attacked Iran's nuclear program and was discovered in 2010," said ESET researcher Anton Cherepanov.

Few Prepared for New Accounting Rule

A new Deloitte survey indicates that many companies are significantly behind in their efforts to implement the Financial Accounting Standards Board's new revenue recognition standard by the Jan. 1, 2018, deadline.

Issued in May 2014, the new standard — Accounting Standard Codification (ASC) 606 —changes the way many companies book revenue, and it will affect all entities that have contracts with customers. Nearly 70 percent of respondents to the Deloitte poll said their organizations are still assessing how they will implement the new standard.

The process has strong implications for IT departments because it involves new ways of collecting, aggregating and reporting data. In most cases, implementing the new standard requires designing and implementing new software solutions and internal controls.

"Implementing the new standard is fast becoming a fire drill," said Deloitte consultant Eric Knachel. "From establishing a budget to ensuring proper data collection and testing system modifications, the implementation process requires substantial time and resources. Companies should not underestimate what a significant undertaking implementation will be."

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.

ProSys locations

Atlanta, GA
(Headquarters)
Phone: 678-268-1300
Toll-Free: 888-337-2626
chash@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
chash@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

Detective Work

SIEM systems help overworked IT teams wade through alerts and event logs to better detect and respond to security incidents.

Common sense would dictate that the longer it takes to discover a security breach, the greater the potential damage. Unfortunately, insider attacks, zero-day exploits and advanced persistent threats are increasingly difficult to detect, giving cybercriminals the advantage of lengthy "dwell times" in compromised systems and networks.

A recent study from Aberdeen Research found that, in half of successful security breaches, the victim organization detected the attack in 38 days or less. In the other half, however, detection took as long as four years, with an average of about 210 days.

The business impact of delayed discovery depends upon the nature of the security incident. The researchers found that organizations can reduce the impact of a data breach by 30 percent if they can cut detection and response times in half compared to the status quo. When it comes to attacks that cause business disruption, organizations can reduce the impact by 70 percent if they can respond twice as fast.

"In multiple areas of cybersecurity, time is currently working in favor of the attackers — and time is the strategic advantage that the defenders need to regain," Derek E.Brink, Aberdeen Vice President and Research Fellow, said in the report.

Security information and event management (SIEM) solutions can aid in the rapid detection of security incidents. SIEM systems correlate security data from across the organization, looking for unusual patterns that could signal a security threat. Data is collected from a wide range of devices and systems in real time, and forwarded to a central console for inspection and analysis.

SIEM helps organizations overcome two of the primary impediments to rapid incident response — an overwhelming amount of security event data and an insufficient number of skilled personnel to analyze it. However, SIEM systems are also complex to configure and manage, which can limit their value.

Searching for Clues

It's easy to see why many cyberattacks go undetected. According to new research from IDC, organizations experience an average of 40 actionable security incidents per week. However, only 27 percent think they are coping comfortably with this workload, while 33 percent describe themselves as "struggling" or "constantly firefighting." More than half (53 percent) say that staff devote too much time to routine operations and incident investigation to improve security response.

"The amount of time companies are spending on analyzing and assessing incidents is a huge problem," said Duncan Brown, associate vice president, security practice, IDC. "The highest paid, most skilled staff are being tied up, impacting the cost and efficiency of security operations. Organizations must ensure that they are using their data effectively to gain key insights quickly to determine cause and minimize impact."

There generally is evidence that an attack is taking place, but it's often buried in log files and alerts that go unnoticed. In fact, so many alerts are generated in the typical environment that IT teams simply can't keep up. A 2015 Ponemon Institute study found that organizations received an average of 16,937 security alerts each week and spent almost 21,000 hours a year analyzing them.

SIEM systems apply data analytics to this monumental task. While a single piece of information has limited value, data collected from multiple systems and viewed holistically can reveal trends and patterns. SIEM systems use statistical correlation to identify relationships between the data points, which are then compared to profiles of

normal system conditions in order to spot anomalies.

While there are a number of solutions to choose from, including both commercial offerings and open source platforms, SIEM is notoriously difficult to implement and manage. Commercial offerings tend to be complex and expensive, while open source tools require significant time and expertise.

Closing the Book

This complexity is reflected in the total cost of ownership for SIEM. According to a recent Ponemon Institute study, the initial purchase of the software represents just 25 percent of the total SIEM cost, with installation, maintenance and staffing making up the remaining 75 percent.

The survey also found widespread dissatisfaction with SIEM. While 84 percent of respondents said their SIEM is important, very important or essential to their incident respondent processes, only 48 percent were happy with the actionable intelligence they get from their SIEMs.

"The root of their dissatisfaction seems to be related to the complexity of the SIEM itself," explained Dr. Larry Ponemon, chairman and founder of the Ponemon Institute. "In fact, 75 percent of respondents said there is significant, or very significant, effort involved in configuring their SIEM. Obviously, this complexity can make it very difficult to extract the value they want and need."

A common complaint is that SIEM is too "noisy" — 54 percent of respondents said that their SIEM generates too much low-level data and too many alerts. Seventy percent want their SIEM to generate fewer alerts that are more accurate, prioritized and meaningful, while 71 percent want to automate certain SIEM-generated tasks so that response teams can focus on priorities.

Increasingly, organizations are engaging managed security service providers to handle the monitoring and management of SIEM. There are also cloud-based solutions that allow organizations to maintain control while eliminating the capital cost and implementation burden of traditional on-premises systems.

SIEM is not a panacea. The Ponemon research revealed that for 65 percent of organizations, the SIEM's discovery of a compromise can take hours, days, weeks or even months. Done right, however, SIEM is a valuable tool that can help organizations regain the strategic advantage of time in detecting and responding to cyberattacks.

Email Evolution

More and more organizations are moving their messaging platforms to the cloud.

Despite the rise of instant messaging, video conferencing and other online collaboration tools, email remains an essential form of communication among business users. According to the "2017 Workplace Productivity and Communications Technology Report" from Webtorials, employees spend 80 minutes per day reading and replying to emails, and ranked email as the most efficient form of communication.

Radicati Group, which conducts an annual study of email trends, predicts that the business email market will continue to grow steadily for the next several years. In its most recent report, the research firm estimates that revenues for business email solutions and services will top $23.8 billion in 2017, and grow to more than $46.8 billion by the end of 2021. That represents an average annual growth rate of 18 percent.

Cloud-based business email solutions are playing a key role in this growth. Smaller organizations are opting for cloud-based solutions because they lack the in-house IT resources to host and manage their email platform. Many midsize and large organizations are migrating their on-premises messaging platforms to the cloud in order to reduce costs and streamline their operations.

The rise of the mobile workforce and geographically dispersed teams is also helping to drive adoption of cloud-based email, which makes it easy to create a common messaging infrastructure regardless of location. In addition, cloud-based messaging makes it cost-effective to extend email to non-office employees, such as retail or factory workers.

Cheaper, Easier

Microsoft Exchange Server is the de facto standard for on-premises email and collaboration services. Introduced in 1996, it was originally called Exchange Server 4.0 because it was offered as an upgrade from Microsoft Mail 3.5. The platform has continued to evolve over the years to address changing business needs and technology requirements.

According to Radicati Group, on-premises Microsoft Exchange still accounts for 68 percent of Exchange mailboxes, with hosted and cloud-based alternatives accounting for just 32 percent. However, the research firm predicts that those numbers will switch by 2021, with on-premises Exchange accounting for just one-third of mailboxes and cloud services accounting for two-thirds.

It comes down to simple economics. Cloud-based Exchange enables organizations to leverage a service provider's infrastructure, eliminating the need to purchase, install, configure and maintain Exchange Server and supporting hardware. Customers purchase email services and storage capacity on a subscription basis, typically a monthly fee per user.

A cloud-based solution can be deployed in a matter of hours, compared to an average of 30 days for an in-house implementation. Users' accounts can be managed easily through a centralized console, even by nontechnical personnel. There's no need to dedicate IT resources to the maintenance and administration of the email platform.

Organizations that have grown through mergers and acquisitions can consolidate their messaging platforms and simplify licensing through a cloud-based solution. And because the service provider is responsible for keeping the environment up-to-date, there are no painful migrations or upgrades as new versions become available.

Choosing the Right Option

Radicati Group defines two primary segments in the cloud-based business email market — Microsoft solutions and Google's G Suite. Microsoft solutions are further broken down into hosted Exchange services and Office 365.

Hosted Exchange services are simply Microsoft Exchange Server deployments that are hosted and managed by a service provider. They offer a certain degree of customization and average 99.999 percent availability. With Office 365, customers always get the latest features and greater integration with other Microsoft products, but there is little to no opportunity for customization and only 99.9 percent guaranteed uptime.

Office 365 and G Suite offer similar functionality, each with its strengths and weaknesses. The choice between Office 365 and G Suite typically comes down to user familiarity with the productivity apps that are bundled into the platform.

Migrating messaging services to the cloud isn't a simple undertaking, particularly for organizations with numerous mailboxes and large volumes of data. The migration process must be carefully planned to avoid business disruption and data loss that could impact data governance and regulatory compliance requirements.

Some organizations remain concerned about the security and privacy of cloud-based business email, but cloud services are often more secure than on-premises platforms. Considering that cloud-based solutions can also cut costs and simplify management, it's easy to see why more and more organizations are getting out of the business of maintaining their own email and turning the process over to a service provider.

NetApp™

Simply scalable storage with NetApp

Eliminate the expense and guesswork of storage provisioning with NetApp OnDemand. With OnDemand, storage is preinstalled and available for immediate use to meet both planned and unplanned capacity requirements. You pay after the fact at a predetermined cost per gigabyte based upon your usage. **Contact ProSys to learn more.**

PROSYS

www.prosysis.com 888-337-2626