March 2014

PROSYS

Tech Outlook

The Next Wave

Software-defined data center promises to take over where server virtualization left off.

Has server virtualization run its course? That's what TheInfoPro predicted recently when it released its latest Servers and Virtualization study. The analyst firm stated that the server virtualization "bubble" has burst, and that while organizations will continue to devote budget dollars to server virtualization projects, such spending would be used to maintain a "steady-state" environment.

It's hard to imagine server virtualization as a "bubble." With roots in the days of mainframes, the technology has been a building block of the modern data center for a decade. Back in 2006, research firm IDC predicted that server virtualization was set to take off, as organizations sought ways to reduce the number of physical servers in the

continued on page 2

TECH OUTLOOK

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

The Next Wave

continued from page 1

data center and break the "one server, one application" requirement.

Since then, virtual machine sprawl is more problematic than physical server sprawl as organizations take advantage of virtualization to rapidly provision new applications and services. About 60 percent of server workloads are virtualized today.

But TheInfoPro's study revealed that IT decision-makers are shifting their attention to the software-defined data center (SDDC), a relatively new concept that many view as the next logical step for virtualization. Coined by VMware CTO Steve Herrod in 2012, the term refers to an environment in which all infrastructure components — including compute, storage, networking and security — are pooled, aggregated and delivered as software. Provisioning, configuration and management of the infrastructure and applications are automated using policy-driven software.

"Management and automation are critical next steps in the evolution of the data center," said Matt Merriman, VP of Professional Services, ProSys. "Organizations are looking beyond server virtualization to solutions that create a more agile, flexible and efficient IT infrastructure. SDDC promises to provide a platform that serves as a bridge to the cloud and enables IT to keep up with the pace of the business."

Extending Benefits

TheInfoPro study found that IT decision-makers are focused less on infrastructure technologies and more on the software needed to run cloud-ready data centers. Thirty percent are planning to increase spending on cloud platforms in 2014, along with management and automation.

"As organizations move beyond virtualization of production workloads, attention is shifting towards the management and automation of the software-defined data center," said Peter ffoulkes, TheInfoPro's Research Director for Servers and Virtualization. "Over the next two years, the foundations for enterprise cloud computing will be deployed with cloud platforms standing out as the hottest technology and the most critical strategic decision to be made."

This change in emphasis comes as the benefits of server virtualization begin to plateau. Server virtualization drives cost savings and improved utilization of compute resources but often increases complexity in other areas of the infrastructure.

For example, many IT departments overprovision storage in anticipation of ever-increasing virtual server demands, resulting in greater management and administration burdens. Organizations must virtualize storage, networking and security in order to improve productivity and efficiency across the data center.

"It no longer takes weeks to turn up a server for a new application — a virtual machine can be provisioned in minutes," Merriman said. "But in most environments, storage, networking and security remain physical rather than virtual. Deployment of the infrastructure needed to support the virtual machines is a lengthy process that drains IT resources. The SDDC removes this bottleneck by virtualizing all infrastructure components, bringing the economic advantages of virtualization to the entire data center."

The SDDC removes bottlenecks by virtualizing all infrastructure components, bringing the economic advantages of virtualization to the entire data center.

Automation speeds application deployment and enables user self-provisioning of applications and services. Application workloads are balanced automatically and moved as needed to meet changing business demands.

By relieving tedious maintenance and management tasks, the SDDC also enables IT to focus on developing innovative solutions. The result is a more efficient, resilient infrastructure

that optimizes resource utilization and maximizes the value of IT investments.

Aligning IT and the Business

SDDC further enables an IT-as-a-Service (ITaaS) model, in which the IT department becomes a business that creates and delivers products and services for other business units.

"SDDC creates the foundation for ITaaS by providing end-users with an on-demand, self-service platform through the automation of service provisioning," said Merriman. "IT establishes policies and manages the environment rather than responding to individual requests for application deployment. IT processes are streamlined, reducing capital and operational costs, improving business agility and making life easier for IT and the organization as a whole."

In a recent IDC survey, 76 percent of organizations said that ITaaS is critical or very important to their success, and SDDC played a key role in enabling the ITaaS model. SDDC makes it possible for IT to define the core architecture and create standardized systems that will deliver both internal and third-party services to users.

Notwithstanding these benefits, SDDC adoption should be approached strategically. Organizations should develop a comprehensive migration plan that identifies the most effective IT structure for creating maximum business value. Certain IT processes may have to change and the impact of SDDC on security, compliance, disaster recovery and capacity planning should be considered.

"IT also deserves a seat at the table with other departments that shape an organization's business strategy," Merriman said. "IT is tied directly to the development and implementation of innovative services and solutions that drive revenue and improve productivity and operational efficiency."

Far from a flash in the pan, server virtualization has helped organizations reduce costs, improve resource utilization and speed application provisioning for a decade. But a new technology is coming to the forefront — not to displace virtualization but to extend it across the data center and optimize it through automation. SDDC promises to capitalize on the benefits of server virtualization and transform the IT department from a technology caretaker to a provider of business services aligned with business priorities.

Tech Outlook

Editorial Correspondence:
7360 E. 38th St.,
Tulsa, OK 74145
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
twheless@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
birminghamsales@prosysis.com

The Carolinas
Phone: 704-560-6053
Toll-Free: 888-337-2626
sbiarsky@prosysis.com

Dallas, TX
Phone: 214-769-9385
Toll Free: 888-337-2626
wbland@prosysis.com

Knoxville, TN
Phone: 865-712-4594
Toll-Free: 800-863-9778
knoxvillesales@prosysis.com

Lexington, KY
Phone: 859-887-1023
Toll-Free: 800-863-9778
dclemmons@prosysis.com

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

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

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

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

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

New York/Metro
Toll Free: 800-634-2588 ext 3
nymetro@prosysis.com

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

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

The Internet of Things

As pervasive connectivity becomes more mainstream, organizations must begin preparing for opportunities and challenges.

In the so-called "Internet of Things (IoT)," billions of objects ranging from automobiles and airplanes to video games and vending machines will be fitted with embedded technology and linked through wired and wireless networks via the Internet Protocol. There is no shortage of hype surrounding the IoT — one tech executive has called it "the biggest business opportunity in the history of people" — but beneath the hyperbole is an undeniable technology trend with far-reaching implications for businesses and consumers.

The possibilities for such technology seem practically limitless, with promising use cases in healthcare, manufacturing, farming, transportation and, well, just about anything you can name. It's no longer merely conceptual, either: the IoT is here, now.

Gartner analysts say the IOT already has nearly 3 billion connected devices and will grow to more than 30 billion by 2020 — and that's not even counting PCs, tablets and smartphones. Gartner predicts IoT will generate $1.9 trillion in global economic value by 2020, while analysts at IDC peg global revenues in the same year at $8.9 billion .

"The momentum of the Internet of Things is driven by a number of factors. There is no doubt that business and consumer demand exists and will continue to expand for IoT solutions," said Vernon Turner, Senior Vice President of IDC's Enterprise Infrastructure, Consumer, Network, Telecom and Sustainability Research. "I expect the current IoT use cases are just the tip of the iceberg."

Blazing the Trail

According to Gartner, industries leading the way in IoT adoption are manufacturing, healthcare and insurance. The firm says the manufacturing sector will benefit from producing billions of devices and from more efficient tracking of materials and components leading to cost efficiencies. In healthcare, smart slippers and other wearable devices contain sensors that detect falls and various medical conditions and can alert a doctor via email or text message if something is amiss. The insurance industry is exploring sensors in cars in order to provide "pay as you drive" insurance that links the insurance premium to the individual's risk profile.

The transportation and logistics sectors are also among early adopters of the technology and could soon move to the forefront of IoT development, according to Frost & Sullivan

analysts. The business consulting firm says the deployment of low-cost, IP-enabled sensors within "things" that move products around as well as within the products themselves creates significant revenue opportunities. For example, the Airbus A380 wide-body airliner has components fitted with sensors to monitor wear and tear in real time. This continually generated data allows Airbus to maintain a dynamic maintenance process and optimize performance.

Development of the IoT has been spurred by a number of factors, including the huge increase in IP addresses enabled by the IPv6 standard. Improvements in wireless networking technology and the greater standardization of communications protocols have also been important, as has the development of low-power, small-core microchips that deliver more processing capabilities for smaller devices.

Security a Concern

Despite these advances, widespread IoT adoption remains inhibited by factors such as a lack of standards, questions about global scalability and a nascent ecosystem for application development. Early adopters also must demonstrate that sensor-driven business models create superior value.

Privacy and security concerns are also significant barriers. In the recent "Georgia Tech Emerging Cyber Threats Report for 2014," university researchers noted that the increase of Internet-capable devices could create huge opportunities for remote hacking and data leakage. With everything from home automation to smartphones and other personal devices becoming connected to the Internet, these devices will capture more real-world information and could permit outside parties, companies and governments to misuse that information.

"Over the next five years, you will see a plethora of devices connected to your home or business network," said

Andrew Howard, a research scientist with the Georgia Tech Research Institute. "And these can be used as avenues for attack."

Because the vast majority of devices will not be complex enough to run sophisticated security software, organizations will need to use network-level monitoring to detect compromises, said Raheem Beyah, associate professor in Georgia Tech's School of Electrical and Computer Engineering.

Really Big Data

Perhaps the biggest challenge of all will be developing the capabilities for capturing, storing, managing, analyzing and retaining the massive amounts of data that will be generated by all of these connected objects. Think "big data" on steroids.

Organizations can't store exabytes or even zettabytes of data in one gigantic data warehouse — information is far more likely to be locked in a variety of different applications and stored as unstructured files. So the first step will be to aggregate the information to be analyzed. Once aggregated, informatics and data science come into play. These disciplines use software and mathematics to discover patterns in the data that humans cannot perceive.

Many analysts say the large-scale data collection and analytics required for the IoT will likely take place in the cloud. Additionally, applications that drive the functionality of sensors and other mobile devices likely will be hosted and developed in the cloud. Amazon recently introduced its Kinesis service to accommodate IoT data growth, describing it as a "fully managed service for real-time processing of streaming data at massive scale." Amazon says Kinesis can collect and process hundreds of terabytes of data per hour from hundreds of thousands of sources.

The Internet of Things is still in its infancy, and it remains to be seen if it will truly become the next great engine of economic growth. However, it is at the very least a disruptive technology that is likely to drive widespread changes and present organizations with numerous challenges and opportunities.

"When the Internet emerged just over two decades ago, it changed everything. But what we're about to see makes that pale in comparison," said John Chambers, chairman and chief executive officer, Cisco.

Asking for Trouble

Lax help desk security puts organizations at risk.

The help desk is where most users turn to resolve IT-related issues. Help desk staff are asked to assist users with password resets, application and connectivity issues, and other common problems. Often the performance of help desk employees is measured by how quickly they can serve callers and resolve the problem.

Unfortunately, security does not play a major role in the process in many cases. As a result, help desks have become an unintended entry point for hackers and malicious insiders attempting to gain access to sensitive enterprise resources through social engineering.

The SANS Institute recently surveyed more than 900 IT professionals worldwide to determine help desk processes, procedures and personnel behaviors that have potential implications for enterprise security. The SANS 2013 Help Desk Security and Privacy Survey found that security technologies are underutilized and nearly 40 percent of respondents have weak or no security policy around their help desks. Only 10 percent of respondents ranked their help desk security practices as robust.

"One thing is clear — successful help desks need to be highly focused on customer service. Yet they can present a security risk for the same reason they are in business — helping a user," said Barb Filkins, SANS Analyst and author of the report. "The only real way to solve the problem is to build security into the business of help desk, from user-friendly but secure self-service tools, to training agents on ways to detect or prevent socially engineered attacks."

Best Practices Lacking

Most respondents (69 percent) identified social engineering as their biggest threat to help desk security. Yet a majority of help desks still verify the identities of callers by requesting personal information such as name, location and employee ID number — information that can easily be used by an imposter. Furthermore, many help desk employees will bypass security controls in an effort to be more helpful to the caller.

Organizations could reduce costs and risk by implementing automated help desk services. Forty-four percent of respondents said

that verifying the identity of call-in users is a much greater threat than that for self-services users (11 percent).

"Self-service tools are viewed as a way to control costs associated with providing help desk services with live, but more expensive, human attendants," said Filkins. "But the success of automation depends on its usability. Online tools can be so convoluted and difficult that an end-user punches '0' to reach the human on the other end, to be led by the hand through the tool's use. Of course, all savings are lost when this happens."

In addition to the human component, lack of training, tools and technology also play- a key role in overall help desk security. More than 51 percent of respondents say they have a moderate approach to help desk security as part of their overall corporate security controls, but are not necessarily focusing on training or additional technologies for day-to-day activities.

Budget Concerns

The good news is that awareness of and training for such attacks exists. More than 70 percent of respondents reported that they are aware of social engineering, and some are even training their help desk staff to be suspicious. The bad news is that organizations are not factoring security into the overall help desk budget.

In most organizations, help desk budgets are determined by the number of users serviced, rather than cost per call or even cost of potential security breaches. Nearly 43 percent of respondents said they do not take the cost of a security incident into account when establishing their help desk budget. As a result, establishing a return on investment for new processes, additional training and tools can be extremely difficult.

Experts at the SANS Institute recommend that organizations provide robust and continuous training for help desk personnel to learn how to spot and react to potential social engineering attacks. In addition, organizations should also consider implementing advanced tools that leverage dynamic data sources and new authentication methods to more accurately identify users and their location. Automation and self-service options for password resets and other common user issues can help reduce errors and vulnerabilities that lead to security breaches and data theft.

The help desk continues to be the preferred method for employees to resolve basic IT issues. Its very charter is to better serve users, making it an attractive target for social engineers and technical hackers attempting to gain entry into networks. In order to close the gap on help desk vulnerabilities, organizations need to rethink their approach to meet the demands of users while protecting against threats.

Tech Support Scams Target Mobile Users

Technical support scams designed to trick unsophisticated computer users into divulging personal information or paying to fix nonexistent problems have recently begun to target smartphone and tablet users, a leading provider of antimalware solutions has found.

Malwarebytes recently described an uptick in scams in which people posing as tech support specialists make unsolicited calls to smartphone and tablet users and attempt to convince them that malware infections or other problems have been detected on their devices. The scammers try to persuade users to download and install remote access programs, which can be used to open various system utilities in an attempt to "prove" the devices have a problem.

Jerome Segura, a senior security researcher at Malwarebytes, documented a case in which a scammer tried to convince him that a harmless system file on his Android device was a "very bad file." The scammer deleted the file, but then used a keyboard shortcut (CTRL+Z) to immediately reinstall it — claiming this was a sign of a regenerating infection. Segura was then advised to buy a 12-month tech support subscription for $299.

"The scary thing is that many people that aren't too tech-savvy will believe these words at face value and end up paying several hundred dollars for dubious services from rogue technical support companies," Segura wrote in a blog post describing the incident.

Microsoft recently issued a consumer alert noting that some scammers are now claiming to represent Microsoft. The firm says users should not trust unsolicited phone calls and should never provide any personal information. Microsoft also offers the following suggestions for anyone receiving a call from someone claiming to be from Microsoft tech support:

- Do not purchase any software or services.
- Ask if there is a fee or subscription associated with the "service." If there is, hang up.
- Never give control of your computer to a third party unless you can confirm that it is a legitimate representative of a computer support team with whom you are already a customer.
- Take the caller's information down and immediately report it to your local authorities.
- Never provide your credit card or financial information to someone claiming to be from Microsoft tech support.

Consumers should also report any suspected attempts at telephone fraud to the Federal Trade Commission by calling 1-877-FTC-HELP or online at http://www.ftccomplaintassistant.gov/.

vmware

Virtualize Everything

Delivering IT as a Service with a Software-Defined Data Center

VMware's software-defined data center infrastructure (SDDC) extends the virtualization concepts you know — abstraction, pooling and automation — to all data center resources and services. SDDC dramatically speeds up and simplifies the initial provisioning and ongoing management of fully virtualized compute, storage and networking by applying powerful policy-driven automation. The result is transformational levels of business agility along with operational efficiency, control and choice for IT and the business alike.

Contact your ProSys representative to learn more.

PROSYS

www.prosysis.com

888-337-2626

vmware PARTNER

PREMIER SERVICE PROVIDER