Tech Outlook

April 2016

With Microsoft Azure and Cisco, organizations gain the agility of the public cloud while maintaining security and control.

Public or private cloud? That's the conundrum organizations have faced as they seek to leverage the flexibility and scalability of the public cloud while addressing security, privacy, performance and availability concerns. The good news is that the cloud is not an "either-or" proposition. Increasingly, organizations are turning to the hybrid cloud model to gain the best of both worlds.

As the name implies, a hybrid cloud uses a combination of public and private cloud services to meet the requirements of various workloads. For example, an organization could use a private cloud to maintain control over mission-critical applications and sensitive data, while leveraging the public cloud for data backup and archival, disaster recovery, and application development and testing.

The benefits of the hybrid cloud are so compelling that it's viewed as the logical end game for most organizations. In a recent study by IDG Research Services, 83 percent of respondents said they currently use or plan to use a hybrid cloud environment, and 73 percent agree that the hybrid cloud model creates a path to digital transformation. The survey found that the hybrid cloud helps increase IT agility by making it faster, easier and less expensive to modernize applications and implement new IT services.

However, the hybrid cloud is complex and cloud services are evolving quickly. The RightScale 2016 State of

continued on page 2

TECH OUTLOOK

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

continued from page 1

the Cloud Report found that lack of expertise is now the top cloud challenge, taking over the No.1 spot from security concerns.

"Resource-constrained IT shops already have a lot on their plates managing traditional in-house infrastructure. The hybrid cloud adds another layer of complexity," said Michael Hritz, Business Development Manager, ProSys. "It's one thing to provision cloud hosting and storage, and quite another to knit together on-premises and cloud infrastructure.

"The choice of cloud platform plays an important role in an organization's ability to tap the benefits of the hybrid cloud. Microsoft Azure, coupled with the Cisco Cloud Architecture, is an intuitive solution that speeds hybrid cloud deployments and makes it easy to optimize workloads across public and private cloud environments."

Combining Forces

The public cloud offers attractive economic and operational benefits, allowing organizations to tap IT infrastructure, applications and services on a pay-per-use basis. However, many organizations are reluctant to place sensitive applications and data in the public cloud. In addition, accessing applications via the Internet brings latency and reliability concerns that make the public cloud unsuitable for many mission-critical workloads.

A private cloud gives organizations the agility of the cloud model in a dedicated, single-tenant environment. Whether deployed onsite or hosted, a private cloud provides control over data center resources while accelerating service deployment and enhancing operational efficiencies.

However, the growing complexity of IT environments makes a hybrid cloud solution the best option in most cases. Organizations can retain control where needed while relying upon cloud service providers for nearly limitless capacity without the associated infrastructure and management overhead.

It's important to note that a hybrid cloud isn't the same as using public and private cloud services simultaneously. In a true hybrid cloud, the public and private clouds are integrated, with a single management interface that makes it easy to move applications and services between the two environments. This eliminates the need to overprovision resources to account for spikes in demand — particularly beneficial for organizations that have highly dynamic workloads.

"This is where the cloud platform comes into play," Hritz said. "In choosing a cloud service provider, many organizations focus on pricing and service-level agreements — which are, of course, important. However, the cloud platform is the operational interface that provides control over compute, storage, networking, security, application and database resources. It's important to consider the depth of infrastructure services and support, as well as monitoring, access control, logging and auditing, and automation features. Application services and data analytics should also be evaluated in certain use cases."

Consistency Is Key

Despite its potential benefits, a hybrid cloud doesn't always deliver ROI. In a survey from The Bunker, nearly two-thirds of CIOs and IT decision-makers said their hybrid cloud deployments failed to meet expectations. Primary reasons were a lack of in-house expertise, poor advice, and a lack of integration of cloud and non-cloud resources.

The Microsoft Azure Stack helps organizations overcome these challenges by bringing Azure cloud services into the private cloud. This creates consistency between the data center and cloud environments, and makes it easy to "burst" services into the cloud as needed during peak periods.

"Azure gives organizations the freedom to choose where their applications should reside while maximizing existing IT investments," said Hritz. "The Microsoft Azure stack incorporates the complete ecosystem of Azure cloud services within a single code base to create a standardized architecture. Organizations can tap Azure's infrastructure-as-a-service and platform-as-a-service features to create a more agile, automated data center."

Azure provides application developers with pre-built templates and an open platform that supports a wide variety of operating systems, programming languages and frameworks. Applications developed using the Azure Stack can easily be moved from the data center to the public cloud.

Because tight integration between the IT infrastructure and application layers is required for cloud service delivery, Microsoft and Cisco developed the Cisco Cloud Architecture for the Microsoft Cloud Platform. The solution combines Windows Azure Pack and Cisco Application Centric Infrastructure (ACI) to enable the rapid delivery of hybrid cloud services. It complements Cisco's OpenStack-based architectures for cloud-native workloads and provides seamless hybrid cloud capability for connecting to Azure.

The appeal of the hybrid cloud lies in its ability to provide cost savings and operational efficiency by allowing organizations to choose the optimal platform for each application and service. However, the challenges associated with integrating public and private clouds have kept organizations from capitalizing on the hybrid cloud.

"Microsoft and Cisco are helping organizations realize the vision of a unified cloud architecture that provides consistency across public and private clouds and streamlines service delivery and management," Hritz said.

News Briefs

Mobile Malware a Growing Threat

The volume of malware targeting users of mobile devices more than tripled in 2015, compared to 2014, according to the annual Mobile Virusology report prepared by the Kaspersky Lab Antimalware Research group. The most dangerous threats were ransomware, a type of malware that restricts access to the infected device and demands payment to the malware operators to remove the restriction.

The report says that 3.8 percent of those using Kaspersky Lab mobile products suffered ransomware attacks in 2015, compared to 1.1 percent in 2014. Attacks were registered in 156 counties, with Russia, Germany and Kazakhstan recording the most instances. The Trojan-Ransom.AndroidOS.Small malware and its modification, Trojan-Ransom.AndroidOS.Small.o were the most active in Russia and Kazakhstan. The Small.o was the most widespread of all mobile ransomware detected by Kaspersky Lab last year.

The report further notes that nearly half of the top 20 Trojans in 2015 were malicious programs displaying intrusive advertising on mobile devices. The most widespread last year were the Fadeb, Leech, Rootnik, Gorpro and Ztorg Trojans.

Some of these apps have the ability to gain super-user access rights or root access. Such rights give attackers an almost unlimited ability to modify information stored on an attacked device. If the installation is successful, the malware becomes almost impossible to delete, even after a reboot to factory settings.

Researchers Develop 'Eternal' Storage

Researchers at the University of Southampton in the U.K. have developed a five-dimensional data storage technique using lasers and nanostructured glass discs to open what they claim could be an era of "eternal data archiving." Scientists from the university's Optoelectronics Research Centre (ORC) say the technique could allow up to 360 terabytes of data to be safely stored at room temperature for nearly 14 billion years.

The technology could allow organizations such as national archives, museums and libraries to preserve their information and records indefinitely on an extremely stable and safe form of portable memory. The technique has already been used to archive historically significant documents such as the Universal Declaration of Human Rights, Newton's Opticks, the Magna Carta and the King James Bible.

The researchers nicknamed the glass discs "Superman crystals" in reference to the "memory crystals" that allow the comic-book superhero to communicate with his ancestors. Data is written to the discs with short, intense bursts of laser light. The self-assembling nanostructures in the glass change the way light travels through it, modifying polarization so that data can be read by a combination of optical microscope and a polarizer similar to that found in polarized sunglasses.

"It is thrilling to think that we have created the technology to preserve documents and information and store it in space for future generations," said Professor Peter Kazansky from the ORC. "This technology can secure the last evidence of our civilization: all we've learned will not be forgotten."

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
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
Toll-Free: 888-337-2626
chash@prosysis.com

Knoxville, TN
Phone: 865-310-8843
Toll-Free: 800-863-9778
pmadden@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
Phone: 425-939-0342
sballantyne@prosysis.com

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

Malware as a Service

New distribution model opens the door to a new wave of cyber security threats.

In popular fiction, movies and television programs, devastating computer network attacks are planned and launched by devious criminal masterminds with extraordinary programming skills, world-class technology assets and limitless financial resources. In real life, it could be anyone with a laptop and a credit card.

A rapidly growing underground marketplace for Malware as a Service (MaaS) is making it easier than ever for anyone to launch cyberattacks. Patterned after the legitimate Software-as-a-Service model, the MaaS market provides easy access to do-it-yourself code kits and botnet computing power necessary for a wide range of targeted attacks. No experience necessary.

In an age when convenience and agility have become essential traits for business applications, it is no real surprise that criminals would value similar qualities. Hacking long ago evolved from teenage hijinks into a high-stakes criminal enterprise in which revenue growth, innovation and market expansion are every bit as important as in legitimate businesses.

"Over the last 10 years, an activity that had typically been carried out by individuals working alone has evolved into an ecosystem of organizations, small groups and freelancers all working together," said Darragh Kelly, product marketer at Bitdefender. "Let's make one point clear – this is a business delivery model within a market, so the main driver is economics."

Market Makers

As in other industries, the new cybercrime model values supply chain efficiency and inventory control. Studies from leading security firms all indicate that MaaS providers boost efficiency by recycling and reusing code, infrastructure and delivery techniques, with periodic modifications to introduce innovation and new functionality.

On the so-called "Dark Web," illicit sites known as cryptomarkets or darknet markets allow criminals to broker transactions involving not only malicious code, but also stolen information such as credit cards and account credentials, as well as a wide range of enablement services such as botnet space, spam services, phishing site design and more. Would-be hackers can obtain full-service packages that makes it easy to launch anything from a DDoS attack to a targeted ransomware attack.

How lucrative is the MaaS market? The underground nature of these operations make that difficult to pin down, but most security experts agree it has to be worth billions of dollars. It is estimated that Russia alone generates more than $2 billion annually in malware profits. According to a Trustwave study, cybercrooks get an estimated 1,425 percent return on investment for exploit kits and ransomware schemes.

In July 2015, an international law enforcement operation led by the FBI dismantled one of the largest darknet markets, known as Darkode. According to law enforcement officials, Darkode provided commercial exploit tools ranging from $300 to zero-day exploits worth millions of dollars. The Justice Department said 20 countries took part in a coordinated operation that led to charges against 12 individuals.

"Of the roughly 800 criminal internet forums worldwide, Darkode represented one of the gravest threats to the

integrity of data on computers in the United States and around the world and was the most sophisticated English-speaking forum for criminal computer hackers in the world," said U.S. Attorney David J. Hickton. "Through this operation, we have dismantled a cyber hornets' nest of criminal hackers which was believed by many, including the hackers themselves, to be impenetrable."

Growing Threat

Unfortunately, the market for as-a-service malware is as strong as ever. Cybersecurity firm Kaspersky Lab has just published extensive research on a MaaS platform that has been the source of attacks on at least 443,000 users and organizations around the world. The malware, called Adwind Remote Access Tool (RAT), is available for purchase online and provides capabilities for remote desktop control, data gathering and data exfiltration. It's available in different versions, and also known as AlienSpy, Frutas, Unrecom, Sockrat, JSocket and jRat.

The malware is written in Java, which means that it can run on Windows, Mac, Linux and Android platforms, and is not readily detected by antivirus tools. Cyber criminals have distributed the malicious code via attachments to phishing emails. If the targeted user opens the attachment, the malware self-installs and attempts to communicate with its command-and-control server.

While it is used mainly by opportunistic attackers and distributed via massive spam campaigns, Adwind has also been used in targeted attacks. During their investigation, the Kaspersky Lab researchers were able to analyze nearly 200 examples of spear-phishing attacks organized by unknown cybercriminals to spread the Adwind malware. Targets of the attacks worked in more than a dozen different industries, ranging from manufacturing and engineering to finance, healthcare, energy, media and government.

Kaspersky Lab researchers estimate that there were around 1,800 users in the Adwind system by the end of 2015, making it one of the biggest malware platforms in existence today. The researchers believe that Adwind customers are scammers who want to use malware for more advanced fraud, unfair competitors, cyber-mercenaries, and private individuals who want to spy on people they know.

Cybersecurity has always been an evolving process, but the MaaS trend is particularly worrisome. By enabling criminals with limited computer skills to launch sophisticated attacks, MaaS sets the stage for significant growth in the scale and frequency of cyber threats. To protect themselves, organizations must guard against complacency, teach users to be vigilant and ensure that up-to-date security tools are in place.

In With the New

A technology refresh can mitigate risks and deliver a boost in performance and efficiency.

Due to ongoing budget constraints, many organizations — particularly smaller businesses — have curtailed technology spending in recent years, choosing to make do with aging systems. These systems generally continue to do an adequate job, but there comes a time when the hard and soft costs of aging equipment outweigh the cost of replacement.

Numerous studies illustrate the overall reluctance to upgrade before absolutely necessary. According to Dimension Data, more than half of business network switches, routers and wireless devices are aging or obsolete. Intel estimates that there are more than 500 million computers in use today that are five years old or older. Corporate360, a marketing data firm, claims that $200 billion worth of tech systems must be refreshed in the next two years.

"Our data shows that organizations are refreshing mostly obsolete devices and are clearly willing to sweat their aging devices for longer than expected," said Andre van Schalkwyk, Consulting Practice Manager for Dimension Data's Networking Business Unit.

Delaying upgrades may conserve capital, but there are risks with such a strategy. The Dimension Data study found a sharp increase in both hardware and software failures with aging gear. These failures, combined with ad hoc troubleshooting and repair practices, can result in extended network downtime and increased operational costs.

End of the Line

End-of-support issues for a number of key technologies signal that it may be time to develop a refresh timetable. In the past year, Microsoft has ended support for Windows Server 2003, SQL Server 2005, the Windows 8 operating system and numerous older versions of Internet Explorer. In addition to potential operational problems, these moves open the door for possible security and compliance issues.

An upgrade to the Windows 10 operating system should be high on the list of priorities. Since Windows 10 was released in July 2015, migration has occurred at a faster rate than any previous version of the Microsoft desktop operating system. Analysts say adoption was sparked by pent-up demand for an OS that would support tablets and 2-in-1 devices following a lukewarm reception to the Windows 8 rollout in 2012. Additionally, free upgrades coupled with broad legacy device support make for a relatively simple transition path.

While older operating systems may seem to offer satisfactory functionality, they are vulnerable because they won't be supported with security patches and upgrades. Some of these older OSs were plagued by gaping security holes anyway, making them favored targets of hackers and a serious threat to the organization.

Several new features make Windows 10 the most secure version of the OS ever. The Device Guard and Credential Guard features protect the core kernel from malware and prevent attackers from remotely taking control of the machine. Device Guard relies upon Windows 10's virtualization-based security to allow only trusted applications to run on devices. Credential Guard protects corporate identities by isolating them in a hardware-based virtual environment.

Windows 10 also offers performance increases, a dramatically improved Web browser, support for virtual desktops, and a number of productivity-enhancing features not found in older versions. It may take a hardware upgrade to realize these benefits, however. Windows 10 simply may not run as well on older systems due to processor speed and memory limitations.

Chip Shots

Intel says the hundreds of millions of older computers still in use are slow to wake, suffer from limited battery life and can't take advantage of all the new experiences available today. The company's new 6th Generation Core processors offer compelling reasons for organizations to consider upgrading PCs and laptops.

Designed for full business productivity, these processors deliver better performance, near-instantaneous wake-up times and significantly longer battery life than previous-generation processors. The product line includes 48 processors across five series to support PCs, All-in-Ones, notebooks, laptops, 2-in-1s and mobile workstations.

The 6th Gen processors help organizations optimize their migration to Windows 10. The chips also promote a more seamless and natural interaction with technology through integration with Cortana, Microsoft's new intelligent personal assistant, and Windows Hello, a biometric login feature.

In addition, the chips give newer hardware a significant security boost. Older PCs that use eight-character passwords have become a virtual front door for hackers — it is estimated that half of all data breaches start with misused or stolen user credentials. The 6th Gen processors feature hardware-enhanced authentication that verifies identities by using a combination of up to three hardened factors based upon company policies. That means organizations no longer have to rely solely upon employees remembering various passwords.

The HCI Edge

Beyond the desktop, industry analysts say data center technology is at the beginning of a new refresh cycle. The Corporate360 survey found that 20 million data center instances of server, storage and networking systems are due for replacement. This is likely to lead to a surge in investments in hyper-converged infrastructure (HCI) solutions that tightly integrate compute, storage, networking and virtualization resources into a single x86-based server deployed in scale-out clusters.

A recent study validated by IDC found that, when compared to traditional infrastructure products, an HCI solution allowed customers to reduce their total cost of ownership by an average of 58 percent, deploy storage up to 85 percent faster and experience up to 98 percent fewer occurrences of unplanned downtime. Given those results, it is no surprise that a whopping 86 percent of respondents to a 451 Research survey said they plan to increase spending on HCI in 2016.

Money is always an important consideration, and IT budgets are likely to remain tight for a while. But for those organizations with computers and servers too old to efficiently handle today's workload or protect against the latest security threats, failure to upgrade could prove to be even more costly in the long run.

Survey: Outdated Technology Costing Businesses $1.8 Trillion

Outdated technology in the workplace does not fit today's modern organization needs, hinders productivity and is creating hidden but significant financial losses for U.S. businesses, according to a new study from Samanage, an enterprise service management software company.

The firm's State of Workplace survey of nearly 3,000 U.S. working adults found that workers spend an average of 520 hours a year on repetitive services and tasks that could be easily automated, including password reset requests, new employee onboarding, contract review and approval, and more. Based on the average national hourly wage of $25.39, this translates to businesses losing $13,202.80 a year, per employee, on unproductive tasks. With a U.S. labor force of more than 140 million, this totals a collective loss of $1.8 trillion annually.

In addition to lost time and money, the survey also found employees are skirting organizational IT policy. More than a third of employees (36.8 percent) say their company's technology is outdated, and one in five workers (18.2 percent) admitted to downloading and using an application without their IT department's knowledge.

The survey results also reveal high demand for productivity-increasing processes and collaboration applications. Survey respondents said automating non-essential tasks (20.2 percent), having access to a more mobile-friendly device (12.2 percent) and using cloud-based apps to access work documents (9.5 percent) would help increase productivity at work.

"Outdated, unproductive technology is burdening U.S. businesses and hurting their employees," said Randy Drawas, chief marketing officer of Samanage. "In order to create a better work life, organizations need to adopt modern technologies that allow them to streamline their internal operations and provide collaborative, easy-to-use technologies that enable employees to spend more time on meaningful and impactful tasks, and far less time on the repetitive and mundane."

Microsoft Azure

The cloud for modern business

Move faster. Save money. Do amazing work.

Microsoft Azure is an open, flexible cloud platform that enables you to build, deploy and manage apps across a global network of Microsoft-managed datacenters. Azure helps you bring products and services to market quickly. You can instantly scale globally, with everything needed to support worldwide business growth. You can run your operations more cost-effectively, paying only for what you use as opposed to for what you don't. You can also free up your budget to spend on other business needs by eliminating the cost of new hardware. And you can gain enterprise-level security with the same data protection and datacenter security that many of the world's largest organizations receive today. **Contact ProSys to learn how Azure can fit your business needs.**

PROSYS
A PIVOT COMPANY

www.prosysis.com
888-337-2626