Tech Outlook

June 2017

PROSYS
A PIVOT COMPANY

The Future of Networking

Cisco software driving transition to smart, programmable and automated networks.

In today's virtualized, cloud-based and mobility-enhanced world, organizations must be able to pivot to new technologies swiftly and efficiently, with minimal disruption and cost. Conventional hardware-centric network infrastructures, in which significant changes can take days or weeks, are no longer suited to meet those requirements.

Gaining that agility can require a fundamental shift in network design philosophy. Increasingly, this means reducing dependence on hardware by virtualizing the entire technology stack — network, compute, storage and security — in what is often referred to as "software-defined everything," or SDx.

"Legacy networks are designed to provide reliable connectivity in a static environment where traffic volume and bandwidth requirements are reasonably predictable," said Michael Hritz, Vendor Alliance Manager, ProSys. "But that predictability is out the window today. Organizations now must support a growing assortment of applications and end-user devices, with data requests coming from anywhere in the world involving a complex collection of in-house and cloud-based data stores.

"SDx creates an agile foundation by abstracting hardware and enabling much higher levels of programmability and automation. It produces a far more fluid environment, removes bottlenecks and unifies what has become a fragmented infrastructure."

Software Shift

Research from IDC suggests organizations around the world will triple

continued on page 2

continued from page 1

their adoption of modern, automated networks over the next two years. Cisco anticipated this trend several years ago and has since developed an impressive portfolio of software solutions designed to accelerate network digitization.

"I am pleased with the progress we are making on the multiyear transformation of our business," said Chuck Robbins, CEO, Cisco. "We are laser-focused on delivering unparalleled value through highly secure, software-defined, automated and intelligent infrastructure."

This transformation was jump-started with the November 2013 introduction of the Application Centric Infrastructure (ACI), Cisco's software-defined networking (SDN) solution that introduced policy-based automation and application delivery acceleration. Cisco revealed a more fully developed strategy with last year's launch of its Digital Network Architecture (DNA).

Cisco DNA extends software-defined principles throughout the entire network, enabling organizations to extend network services from the campus to the branch, whether the network is wired or wireless, at the core or at the edge. Delivered through the company's cloud-based Cisco ONE software portfolio, the platform enables SDN functions along with network functions virtualization (NFV), model-driven programming, overlay networks, open APIs, cloud management, orchestration, analytics and more.

DNA Strands

A key element of DNA is Evolved Cisco IOS XE, an operating system optimized for programmability, controller-based automation and serviceability. The OS provides open model-driven APIs for third-party application development, software-defined management, application hosting, edge computing and abstraction from the physical infrastructure to enable virtualization.

An NFV engine that optimizes the delivery of network services through virtualization and consolidation is included in the OS. Enterprise NFV virtualizes functions such as routing, firewall, WAN optimization, WLAN controller and orchestration.

The network perimeter is the gateway to the Internet, but traditional, static network perimeters are struggling with the new realities of the digital era. The Secure Agile Exchange solution virtualizes the network perimeter and extends it to colocation centers. This allows organizations to dynamically connect customers, employees and partners using on-demand, virtualized network services.

Growth of the Internet of Things is bringing special challenges to the perimeter. Cisco DNA includes security features designed to improve visibility into devices, endpoints and applications. Identity Services Engine (ISE) 2.2 dynamically controls network access, assesses vulnerabilities and applies threat intelligence. It can also contain suspicious devices for remediation.

Cisco TrustSec provides software-defined segmentation that isolates attacks and restricts movement of threats anywhere on the network, from the edge to the data center and cloud. This dynamic segmentation makes security policy changes 98 percent faster than traditional methods, with an 80 percent reduction in operational efforts.

Recent Acquisitions

Cisco added to its SDx portfolio with the recent acquisition of Viptela, which specializes in software-defined wide-area network (SD-WAN) technology. Viptela is known for its innovative virtual routers that can be deployed in a variety of private, public and hybrid cloud computing environments and are supported on all major hypervisor platforms.

"Cisco already has two other SD-WAN solutions — Intelligent WAN (iWAN) and Meraki SD-WAN — but those are cloud-managed solutions that work with installed hardware," said Hritz. "Viptela is a pure-play, software-defined option, which aligns perfectly with Cisco DNA."

Another recent purchase hints at Cisco's road map for network automation. MindMeld developed a unique artificial intelligence (AI) platform that enables customers to build intelligent and human-like conversational interfaces for any application or device. Through its proprietary machine learning (ML) technology, MindMeld delivers incredible accuracy to help users interact with voice and chat assistants in a more natural way.

In the short term, Cisco will no doubt incorporate this AI technology with its Spark collaboration suite, allowing natural language commands for its team messaging and conferencing tools. Beyond that, Cisco has indicated it intends to embed AI and ML capabilities across the network and the cloud with the goal of creating self-managed networks.

"It's a natural progression," said Hritz. "Artificial intelligence and machine learning applications gather data, interpret it and learn from it. It's easy to imagine using AI to monitor the behavior of your virtual machines and the applications running on your network. AI could also help you identify new security threats, improve predictive analytics, optimize data streams and more."

There was a time when Cisco became the most valuable company in the world by selling networking hardware. However, network requirements have evolved rapidly, requiring a shift from static legacy systems to flexible, programmable platforms with the intelligence to allocate resources dynamically. Cisco has evolved as well, developing comprehensive software solutions that enable the digital-ready network.

News Briefs

Companies Eye Software-Defined Storage

Traditional enterprise storage strategies may not be keeping up with the exponential growth of business data and are under the microscope in 70 percent of IT organizations, according to a recent study commissioned and released by open source infrastructure solution provider SUSE.

The study found the vast majority of companies have revised their storage approach and strategy in the last 12 months due to frustrations associated with storage costs, performance, complexity and fragmentation of existing solutions. A majority of them are looking at software-defined storage to help bridge the gap.

An overwhelming majority of companies – 95 percent – are reporting interest in the scalability and efficiency of software-defined storage. Sixty-three percent say they will begin to adopt a software-defined storage approach in the next year.

Eighty percent of all respondents report frustration with the cost of their current storage system, 92 percent are worried about managing storage costs as capacity requirements grow and 71 percent said storage systems were complex and highly fragmented. As a result, companies' most commonly reported priority in the next 12 months is to simplify their storage approach.

FTC Says Phishing Defenses Lacking

Most major online businesses are using proper email authentication to prevent phishing emails but few of these businesses are taking full advantage of the latest technologies to combat phishing, according to a new study from the Federal Trade Commission (FTC) Office of Technology Research and Investigation.

Phishing is a type of online scam that targets consumers by sending them an e-mail that appears to be from a well-known source such as an Internet service provider (ISP), a bank or a mortgage company. It asks the consumer to provide personal identifying information, which the scammer then uses to open new accounts or invade the consumer's existing accounts.

Specifically, the study found that 86 percent of the major online businesses it studied are using Sender Policy Framework (SPF), an email authentication technology that enables ISPs to determine whether messages that claim to be from a business' email addresses actually come from the business.

Fewer than 10 percent of the businesses, however, have implemented a supplemental technology known as Domain Message Authentication Reporting and Conformance (DMARC) in a manner that would allow the businesses to receive intelligence on potential spoofing attempts and to instruct ISPs to automatically reject any unauthenticated messages that claimed to be from the businesses' email addresses. By using DMARC to instruct receiving ISPs to reject unauthenticated messages, online businesses could further combat phishing by keeping these scam emails from showing up in consumers' inboxes.

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

Protecting Sensitive Data

Encryption is the key to minimizing the risk of embarrassing and costly security breaches.

A seemingly endless list of high-profile data breaches has organizations worried about the threats posed by hackers. The ongoing adoption of cloud applications and storage brings concerns about the security of data on third-party systems. And more and more employees are transmitting and storing sensitive information on mobile devices — devices that could be lost, stolen or compromised.

Each of these security risks raises the specter of a data breach, one of the most costly and potentially devastating threats organizations face. The loss or exposure of sensitive information exacts an enormous price, including the costs of investigating and recovering from the breach, notifying affected individuals, lost productivity, legal fees, regulatory fines and brand damage.

While there is no foolproof way to prevent a data breach, one technique comes very close: encryption. Encryption effectively "scrambles" data, which cannot be read without access to the correct encryption key. As a result, encryption can dramatically reduce, if not eliminate, the security risks associated with the loss or theft of data.

According to the 2016 Encryption Applications Trends Study conducted by the Ponemon Institute, the use of encryption is on the rise. Companies that report using encryption extensive-

ly jumped 7 percent to a total of 41 percent, the largest increase in the 11-year history of this report.

"There has been a steady increase in the use of encryption technology, with the highest increase ever in this year's results," said Dr. Larry Ponemon, chairman and founder of The Ponemon Institute. "Along with that increase we've seen the rise of new challenges in the areas of encryption key management, data discovery and cloud-based data storage. The findings of this study demonstrate the importance of both encryption and key management across a wide range of industries and core enterprise applications."

Growing Requirement

Organizations in certain regulated industries have very real incentives to encrypt data. The Health Insurance Portability and Accountability Act (HIPAA) requires covered entities to provide notice to affected individuals, the Department of Health and Human Services and in some cases the media if there is a breach of unprotected data — that is, data that is not encrypted.

The healthcare sector isn't the only industry that promotes encryption. Under California's Security Breach information Act and similar regulations enacted by other states, companies must disclose even suspected security breaches to the media and all individuals potentially affected. Encrypted data is exempt, however.

The Payment Card Industry Data Security Standard (PCI DSS) mandates the encryption of stored data, including data on backup tapes, as well as point-to-point encryption of data from the point of interaction until the data reaches the payment gateway, processor or acquirer. The latest versions of PCI DSS require that merchants migrate from older, insecure cryptographic technologies, a transition that must be completed by June 30, 2018.

It's hardly surprising, then, that organizations in the financial services, healthcare and pharmaceutical, and technology and software sectors are using encryption the most, according to the Ponemon study. This indicates the influence of regulations and privacy concerns on the need to protect against data breaches.

Many organizations still operate under the assumption that encryption saps productivity, makes finding and retrieving information more difficult, and increases the complexity of storage and backup processes. Indeed, older encryption solutions required companies to make painful tradeoffs to achieve data security: performance degradation, operating system and application dependency or changes in workflow. However, encryption systems can be configured in ways that minimize performance problems, and newer technologies are more flexible and require fewer resources.

Locking It Down

Encryption key management is another major pain point. Cumbersome manual processes are often used to generate, distribute, secure, expire and rotate the encryption keys used to scramble and unscramble data. This results in increased costs for IT, difficulty meeting audit and compliance requirements, and inaccessible data if keys are lost.

Organizations should take a policy-based approach to encryption key management, governing access to keys, sharing of keys, expiration of keys, shredding of keys, and all other aspects of key lifecycle management. Encryption key management solutions help to enforce policies while making it easier to create and control the master keys used for various types of applications and data. In addition to traditional hardware security modules — physical devices that safeguard and manage encryption keys —cloud-based offerings as well as hybrid cloud and on-premises products are becoming widely available.

The latest versions of the Payment Card Industry Data Security Standard require that merchants migrate from older, insecure cryptographic technologies, a transition that must be completed by June 30, 2018.

Some encryption appliances perform their own key management. For example, email encryption solutions will retrieve the appropriate key so that the recipient can unlock and read an encrypted email. Similar products can be used for other types of applications as well.

Enterprise-wide encryption solutions automatically encrypt data when it's created, ensuring the security of data when it is emailed or shared across platforms and devices. While encryption is transparent to the user, decryption requires user action, helping to prevent accidental data leakage. Decryption activities are logged and administrators are alerted if someone attempts to decrypt a large number of files.

Recent data breach incidents and growing security threats have led more organizations to encrypt data within the data center, on endpoint devices and at all points in between. Modern encryption and key management solutions can effectively eliminate the risk of a data breach without disrupting workflows or impacting productivity.

Finding the Value of UC

Making the case for upgrading an aging phone system.

Although IP-based telephony has been providing organizations with documented benefits for going on two decades now, a surprisingly large number of companies still depend on legacy time-division multiplexing (TDM) services. Nemertes Research says more than 70 percent of companies still use TDM, although most at least have IP in the mix.

While it's only natural to want to squeeze every dollar of value out of technology investments, this may not be the wisest strategy when it comes to aging phone infrastructure. With a push from the Federal Communications Commission, major carriers are actively transitioning from TDM circuits to IP networks. Companies clinging to older infrastructure will face rising maintenance costs and heightened risk of failure.

Beyond the hard costs of service and support, aging phones also have significant opportunity costs — particularly if they are impeding digital transformation initiatives. Outdated features, limited mobility capabilities and fragmented applications create quality and operational issues that restrict productivity, inhibit innovation and frustrate customers.

Enabling Transformation

IP-based unified communications (UC) platforms lay the groundwork for digital transformation by synchronizing an array of communications and collaboration tools, and by enabling broader integration with key business applications. This helps create an agile, engaged and connected workforce through the delivery of a consistent, reliable communications experience across multiple devices and locations.

Global Market Insights predicts the UC market will grow to $96 billion by 2023 as organizations increasingly realize the value of updating their communications infrastructure. While increased functionality is the major driver, cost is another consideration. UC adoption has trailed expectations for most of the past decade, in large part due to perceived high capital costs for the acquisition of hardware, software and endpoint devices. That perception is shifting, however. Nemertes says capital costs should no longer have much bearing on the UC decision.

The research firm conducts an annual analysis of real-world UC expenses, with an emphasis on total cost of ownership (TCO) based on three categories — capital investments, implementation costs and operational expenses. According to the firm's most recent report, year-over-year UC capital costs have dropped by 25 percent due to increased competition in the market and growing adoption of cloud-based solutions.

The Cloud Option

The cloud-based UC-as-a-Service (UCaaS) delivery model is on the rise, largely because it shifts acquisition costs and internal staffing burdens to a provider. Nemertes found that in 2016, more than half of organizations with UC have adopted cloud services, compared to just 26 percent in 2015.

Interestingly, Nemertes finds that UCaaS can have slightly higher ongoing operational costs than on-premises deployments. Follow-up interviews revealed this is often because organizations tend to limit ongoing training and engineering expenses once a system is in place. Conversely, those with cloud-based services tend to continue training and expanding usage to ensure they are getting the most bang for their buck.

In light of these market dynamics and to better reflect the importance of ongoing operational costs, Nemertes is now calling TCO "total cost of operations" rather than "total cost of ownership." The firm says implementation costs increased 60 percent year-over-year while operational costs increased 21 percent. In many cases, however, these cost increases are the result of the new emphasis on UC's broader collaboration features.

Elements such as robust mobile clients, enterprise-grade videoconferencing, document-based collaboration and social media integration have greater network overhead than basic UC apps such as email and instant messaging. The integration of voice, video and messaging functionality directly into business applications also adds complexity. While these features add costs, they also provide improvements in processes and productivity that are difficult to quantify.

Businesses today require multiple communications technologies to operate effectively. IP-based unified communications systems can integrate, coordinate and manage those technologies for maximum benefit. With so much at stake, those considering a UC system should avoid the temptation to make a decision based solely on upfront costs. By looking at the big picture and analyzing long-term operational costs, organizations will be able to calculate TCO and make the smartest possible decision.

Accelerate Digital Network Transformation with Cisco DNA

Build a digital-ready network that is simple, automated, intelligent and secure with Cisco Digital Network Architecture. Cisco DNA is an open, extensible and software-driven architecture designed for automation to make network services easy to deploy, manage and maintain — fundamentally changing the approach to network management. Cisco DNA allows you to virtualize your entire technology stack, giving you the freedom to run any service anywhere, independent of the underlying platform — physical or virtual, on premises or in the cloud. **Contact ProSys to learn more about digitizing your network with Cisco DNA.**

PROSYS
A PIVOT COMPANY

www.prosysis.com 888-337-2626