May 2014

PROSYS

Tech Outlook

Keys to the Kingdom

Cisco Identity Services Engine allows employees to work when, where and how they want, on the devices they want — without compromising security.

Medieval security might seem primitive by today's standards, but it was quite effective in its day. Castles were surrounded by a high wall and moat (dragon optional), and a sentry was posted at the gate to demand the identity of a visitor before lowering the drawbridge. This protected the castle from attack while permitting the comings and goings needed for the day-to-day operation of a kingdom.

Modern-day firewalls have supplanted the castle wall and moat, keeping out most of the network traffic that may pose a threat to the organization. However, organizations still need a sentry that allows users to access the resources they need to conduct the organization's business. That is the function of identity and access management (IAM) solutions.

"IAM has become increasingly important given mounting security threats and regulatory compliance concerns," said Matt Merriman, VP of Professional Services, ProSys. "Many organizations are also embracing the Bring Your Own Device concept as a way to stop managing end-user hardware and

continued on page 2

TECH OUTLOOK

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

Keys to the Kingdom

continued from page 1

satisfy user demands. However, the rapid influx of employee-owned mobile devices makes it difficult to ensure robust security as well as a seamless user experience.

"The Cisco Identity Services Engine supports and enables BYOD by allowing role-based access to appropriate services from any device. Cisco ISE gathers information from the network, users and devices in real time, then uses this information to make proactive, context-aware governance decisions."

Uniform Policy Enforcement

IAM is about more than simply assigning access privileges — it governs how those privileges change over time and in various situations. With users leveraging cloud services, social networks and enterprise systems in a wide range of circumstances, IT must be able to enforce access policies across the organization.

"Employees want to use their own devices at work, as well as have more flexibility as to when, where and how they work," said Merriman. "At the same time, 70 percent of employees admit they break IT policies, with 20 percent citing the need to access unauthorized programs and applications to get their jobs done. Clearly, unified policy enforcement is needed to create a secure work experience that supports both employee and IT needs."

Cisco ISE delivers unified policy enforcement across the enterprise. As the centralized policy engine for the Cisco TrustSec Solution Architecture, it enables organizations to efficiently set specific policies based on users' roles, the security posture of the devices they are using, their location, and the network resources they need to access. It solves the "any device" challenge by enforcing access policies across wired and wireless LANs, cellular networks and VPN connections.

"Cisco ISE can distinguish between organization-owned and user-owned devices and automate security across the organization with network-enforced access policies and encryption," Merriman said. "It simplifies IT operations by enabling policy definitions that mirror business rules."

Complete Visibility and Control

Using fine-grained controls that combine context awareness, identity awareness, policy and threat intelligence, Cisco ISE delivers a powerful combination that helps organizations deliver the right levels of security in all segments of their network. It provides all the services required for access control — authentication, authorization and accounting (AAA), profiling, posture and guest management — in one powerful solution that increases IT efficiency and improves compliance. It also serves as the "single source of truth" for context-based identity attributes, including device, location and security posture.

Cisco TrustSec and ISE provide comprehensive visibility via device sensors that are integrated into the infrastructure to automatically detect and classify all devices attaching to the network. Cisco ISE also provides real-time directed endpoint scans, based on policy, to gain more relevant insight and accuracy while classifying devices. Together, they provide the industry's most scalable, reliable and comprehensive view of mobile devices across an entire corporate infrastructure.

"Cisco ISE enables organizations to accommodate an increasingly mobile workforce without increasing the burden on the IT team," said Merriman. "It includes zero-touch onboarding, which guides users through an easy, step-by-step process to quickly self-provision their devices at a time that's most convenient for them. Sponsor-driven guest access, automatic device classification, auto endpoint onboarding and portal-driven device registration allow IT to focus on more complex, time-sensitive matters while giving users greater flexibility."

In our next issue:

GOING GLOBAL

Learn how ProSys is helping its clients with international IT requirements, including networking, virtualization and storage solutions for data centers.

Flexible Solution

Cisco ISE can be deployed as a physical or virtual appliance that integrates with existing Cisco network devices and directory services. ProSys has completed rigorous training in the Cisco TrustSec Solution Architecture, and has demonstrated success deploying the Cisco ISE solution.

Innovative licensing allows customers to choose the functionality they need based upon the number of active endpoints on the network. The Base License provides AAA services, guest lifecycle management and link encryption, while the Advanced license adds automated device onboarding, device profiling, MDM integration and other services. The Wireless license provides both Base and Advanced features for wireless endpoints only.

In medieval times, security was achieved through stout fortifications and a single point of access. Today, organizations must create a flexible and scalable security environment that supports user access anytime, anywhere, using any device.

"BYOD isn't just about connecting user-owned devices and allowing guest access to the network. It's about how you control and secure those connections across the enterprise," Merriman said. "ProSys is helping customers develop a comprehensive BYOD strategy based upon unified policy enforcement, simplified management and an uncompromised user experience.

"Cisco ISE provides organizations with a comprehensive, policy-based approach designed to support the BYOD phenomenon today and tomorrow. Cisco ISE enables organizations to accommodate an ever-growing array of consumer IT devices without sacrificing security and control."

News Briefs

Software Bloat Straining Infrastructure

A tangled web of applications within international organizations is getting more and more complex, putting strain on the IT department and stunting digital transformation, according to a new study from consulting firm Capgemini.

Some 48 percent of 1,116 CIOs and senior IT executives said their companies have more applications than required to run the business. Nearly three-quarters (73 percent) believe that at least one-fifth of their current applications share similar functionality and should be consolidated, and 57 percent believe that at least one-fifth of their applications should be retired or replaced.

This isn't just an IT problem, it's a business problem. As organizations implement new cloud, mobility and big data solutions, they often lack the bandwidth to gain full competitive advantage from these technologies because of the bloated applications landscape.

"In a world where all facets of an organization are starting to embrace digital transformation — and are dependent on the quick deployment of mobile, social, big data and cloud solutions for competitive advantage — a well-rationalized applications landscape suddenly becomes a much bigger, strategic imperative for the whole company," said Ron Tolido, CTO Application Services Continental Europe at Capgemini.

EHR Market Growth Slow but Steady

Despite slower-than-expected growth, the global market for electronic health records (EHR) is estimated to reach $22.3 billion by the end of 2015, with the North American market projected to account for 47 percent ($10.1 billion), according to research by Accenture.

The global management consulting firm says the EHR market is projected to grow 5.5 percent annually through 2015 — a dip from roughly 9 percent growth during 2010. Driven by consolidation and the federal Meaningful Use guidelines, the U.S. is expected to remain the largest EHR market in the Americas and globally, with a projected annual growth rate of 7.1 percent and total revenues of $9.3 billion by the end of 2015.

"Although the market is growing, the ability of healthcare leaders to achieve sustained outcomes and proven returns on their investments pose a significant challenge to the adoption of electronic health records," said Kaveh Safavi, global managing director of Accenture Health. "However, as market needs continue to change, we're beginning to see innovative solutions emerge that can better adapt and scale electronic health records to meet the needs of specific patient populations as well as the business needs of health systems."

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

Counting Costs

Consider many metrics when evaluating TCO of unified communications systems.

The modern workforce has a multitude of business communication and collaboration tools at its disposal, but many of these key tools still tend to exist independently of each other. IP-based unified communications (UC) systems unite telephony, email, voicemail, messaging, mobility, conferencing and more into a single, coherent communications solution.

Although UC systems have been around for nearly 10 years, adoption rates have never really met expectations. A 2013 survey by the IT education company Webtorials found that only 21 percent of companies had fully adopted unified communications.

Sticker shock has been one obstacle to UC adoption. As with any shift to new technology, there are significant upfront costs involved in the move to an IP-based communication infrastructure. Whether organizations are making their first move into Voice over IP (VoIP) or upgrading to a fully integrated UC platform, the shift often involves considerable hardware and software purchases.

However, organizations must be careful that their focus on price does not make them blind to value. In a

benchmarking study of the total cost of ownership (TCO) for unified communications, Aberdeen Group analysts found that buyers typically place too much emphasis on upfront cost when evaluating UC systems and vendors.

The Big Picture

While procurement and implementation costs certainly need to factor into the equation, this approach fails to take into account potential long-term operational, maintenance and network savings that can easily offset upfront costs. Aberdeen recommends a more thorough analysis of TCO metrics to establish a clear cost structure.

"Total cost of ownership represents a holistic measure of the complete financial impact associated with the unified communications purchase decision and should be the most important issue for any IT financial stakeholder purchasing a new system," said Hyoun Park, Aberdeen research analyst. "To uphold corporate fiscal and governance responsibilities, decision-makers must fully examine all significant upfront and recurring costs to identify the UC solution offering the greatest value throughout the entire lifespan of the solution."

Even if the goal is to simply reduce communications costs, organizations must consider all factors that impact TCO. To build an accurate TCO calculation, it's important to look beyond the sales proposal in order to balance the short-term costs with long-term operational savings.

Factors to Consider

The 2013 Nemertes Research benchmarking study of IP telephony TCO separates cost data into three categories:

- **Capital:** Includes servers and other data center hardware, software licenses, and desk phones or other endpoint devices.
- **Implementation:** Includes internal staff time and third-party systems integrators and consultants.
- **Operational:** Includes staff time, training and certification plus maintenance contracts and third-party support.

The Nemertes study suggests that product and implementation costs are generally known and fairly consistent, while operational costs can vary significantly from vendor to vendor. Buyers need to evaluate real-world data related to implementation and operations to calculate TCO. For example, a hybrid system with inexpensive digital phones might reduce upfront costs but could wind up limiting access to the full range of UC solutions and benefits.

Even basic UC systems should provide voicemail, email, unified messaging, and web and audio conferencing as components. However, organizations must consider if they are willing to incur higher upfront costs to gain access to emerging components may well be mission-critical in the near future. These elements include a robust mobile client, enterprise-grade videoconferencing, document-based collaboration and social media integration.

Complexity is another important TCO consideration. Mobility, collaboration and videoconferencing applications have greater network overhead than apps such as email and instant messaging. The increased network engineering and monitoring requirements result in increased TCO.

Network readiness also must be evaluated. Implementing VoIP may require upgrades to improve bandwidth and server resources. A poor network design could negate many of the benefits an organization expects to realize from UC.

The Value Proposition

While a host of factors can impact the cost of a UC deployment, organizations must also have a good understanding of the potential value. Long-distance savings has always been one of the chief selling points of IP communications, and while that can be significant in some organizations, it isn't the only way VoIP and UC deliver value. An IP-based system with centralized call control can also reduce trunking, maintenance and staffing costs.

Improvements in processes and productivity may be harder to quantify but are significant nonetheless. A recent survey sponsored by Sonus Networks attempted to identify those savings. Technology decision-makers at 267 large enterprise organizations responded that a fully functional UC infrastructure could improve productivity of selected tasks by 23 percent. By recovering 1.21 hours per employee per day, the average savings is roughly $13,000 per year per knowledge worker employee.

"Our communication modes have been discrete for too long, and the opportunity to bring them together to drive personal productivity is immense," said Wes Durow, Sonus marketing VP.

Businesses today require multiple communications technologies to operate effectively. VoIP-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.

Next-Gen Firewalls

Application awareness and other smart features change the game for network security.

Using a traditional firewall against modern security threats is like playing professional football in the 21st century with an old leather helmet from the 1930s. It may provide some very basic protection, but it isn't strong enough to prevent serious or even permanent damage.

Traditional firewalls provide security by inspecting and controlling traffic according to specific ports, protocols and IP addresses. That was effective when most network threats involved hackers scanning for open ports on network firewalls to attack. Today's threats are far more stealthy and sophisticated.

Many modern cyber threats are designed to piggyback on legitimate application-layer network traffic, which allows their malicious payloads to bypass stateful packet inspection mechanisms. More than viruses and spyware, modern security threats include zero-day exploits, advanced malware and stealth bots that are smart enough to not only disable security protections and steal data, but hide in the network while awaiting further instructions.

Just like football gear, however, firewalls have evolved. Next-generation firewalls (NGFW) offer a much more robust line of defense.

Understanding Apps

Along with traditional firewall capabilities such as packet filtering, network address translation and URL blocking, NGFW integrate many more robust features. These include intrusion prevention, Secure Socket Layer (SSL) and Secure Shell (SSH) inspection, deep-packet inspection and reputation-based malware detection.

However, the key distinction is that an NGFW is application-aware, meaning it can distinguish one application from another and enforce granular security policies at the application layer. With the ability to understand details of web application traffic, the NGFW can make smarter blocking decisions based upon very specific criteria. That is a critical capability, considering that secu-

rity experts estimate that 80 percent of attacks today happen at the application layer.

"Big security news stories are a daily event as the threats facing enterprises are getting more pervasive and sophisticated," said Jeff Wilson, principal security analyst with Infonetics Research. "Organizations need to implement protections against advanced application-layer threats throughout their networks – not just at the edge."

The change in business environment due to the Bring Your Own Device (BYOD) model, cloud-based services and wireless communication has also created new threat vectors. Employees today expect to gain network access with their mobile devices and use cloud-based solutions to work with company data. According to a recent Network World study, 48 percent of respondents said that supporting increasing numbers of mobile devices is their organizations' top security challenge.

Although mobile devices connect to the Internet from outside the corporate firewall, it is possible to backhaul remote and mobile traffic to a corporate site for NGFW inspection. Even without taking this step, organizations gain some essential security measures for the mobile/cloud environment. For instance, an NGFW decrypts and removes hidden threats from mobile traffic tunneled over SSL VPNs before they enter the network. NGFW appliances can also be configured to limit general access to cloud file transfer applications.

Be Prepared

An NGFW is sometimes confused with a unified threat management (UTM) system, which combines various security functions — firewalls, antimalware software, intrusion protection, content filtering, reporting and more — in a single security appliance. Truly comprehensive network security can be achieved when employing both of these complementary systems.

When choosing an NGFW, organizations must evaluate the architecture, performance impact and manageability. Whether choosing a hardware- or software-based solution, it is important to understand how the product is engineered and how it will be integrated with existing infrastructure.

The additional features and options offered by an NGFW could eliminate the need for some individual security devices, which could reduce operational expenses. However, those additional features also require very specific policies and rules, so the best NGFW is one that is intuitive and easy to configure, implement and maintain. Simple, centralized management is critical.

Next-generation firewalls are the logical evolution in network security and access control. Organizations that have not already done so should make plans to migrate to NGFW technology. It's the best way to avoid the risk of game-changing security threats due to substandard protection.

Secure Access for Wired, Wireless and VPN

Cisco Identity Services Engine (ISE) gives you a single policy control point for the entire enterprise, enabling secure wired, wireless and VPN connectivity. Cisco ISE is used to provide secure access and guest access, support BYOD initiatives, and enforce usage policies. Cisco ISE is designed to support up to 250,000 active, concurrent endpoints – more than any other product in the marketplace – to ensure seamless onboarding, roaming, and network access control throughout a distributed enterprise network.

Contact ProSys to learn more.

PROSYS

www.prosysis.com 888-337-2626

Gold Partner