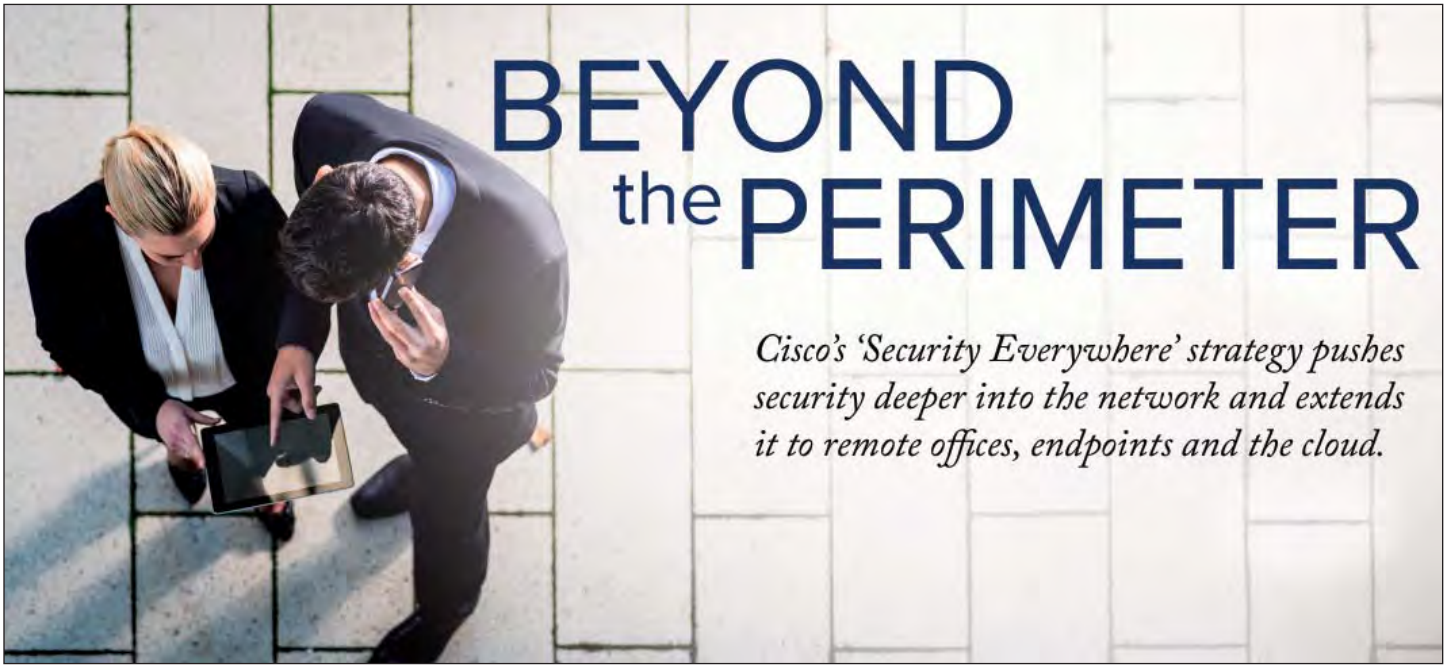
Tech Outlook

January 2016

PROSYS
A PIVOT COMPANY



BEYOND the PERIMETER

Cisco's 'Security Everywhere' strategy pushes security deeper into the network and extends it to remote offices, endpoints and the cloud.

For years now, organizations have been opening up their networks to remote and mobile workers, customers and business partners. They've been adopting web-based applications and cloud-computing models. The days of the "closed" network are over.

While this environment offers many competitive advantages, it also increases security risks. Cybercriminals no longer scan for open ports on network firewalls to attack — they have far more sophisticated attack methods and more choices of attack vectors. Once inside the network, they often remain undetected for long periods of time, accessing systems and stealing sensitive data. In many cases, organizations do not detect this activity until it's too late.

"In today's threat environment, security must be extended far beyond the traditional network perimeter — users, data and applications have to be protected wherever they are," said Michael Hritz, Vendor Alliance Manager for ProSys. "Traditionally, that meant assembling a complex array of point solutions that are not interoperable and leave serious security gaps. IT teams lack visibility into potential threats, making detection and remediation more difficult."

Recognizing these challenges, Cisco has developed one of the industry's most comprehensive threat protection portfolios, encompassing an array of

continued on page 2

TECH OUTLOOK

continued from page 1

advanced products and solutions covering the broadest range of attack vectors throughout the attack continuum. With its new "Security Everywhere" strategy, Cisco is integrating many of these solutions and embedding them throughout the extended network to make network security more pervasive and less complex than ever before.

"Cisco's Security Everywhere approach is designed to address customers' security challenges across their entire IT infrastructure. This expanded portfolio of security solutions provides greater visibility, context and control from the data center out to endpoints, branch offices and the cloud," Hritz said.

The Network Is the Security Device

There has been a 66 percent compound annual growth rate in detected security incidents over the past six years, according to the Cisco 2015 Annual Security Report. Data from this report indicates that malware is becoming increasingly sophisticated and cybercriminals are becoming stealthier and better organized with an abundance of resources at their disposal.

At the same time, the attack surface is expanding dramatically as the Internet of Everything continues to grow. According to the 2015 Cisco Visual Networking Index Forecast, the number of IP-connected devices and machine-to-machine connections will increase from 14 billion in 2014 to more than 24 billion by 2019.

"Cisco is addressing this trend by adding more sensors to network devices, creating a pervasive threat protection environment that helps organizations close the gaps in their defenses," said Hritz. "The network becomes the security device, making it possible to rapidly identify anomalies and misuse of the network or applications."

The embedded security capabilities also enhance automation, enabling organizations to dynamically enforce security policies and reduce threat detection and response times. Applications and users can be segmented throughout the network and suspicious devices or activity rapidly blocked.

These capabilities are enabled by broad integration between Cisco's Identity Services Engine (ISE) and TrustSec software-defined segmentation and Lancope's StealthWatch threat detection and analysis solution. Organizations can go beyond mapping IP addresses to identifying threat vectors based upon ISE's context of who, what, where, when and how users and devices are connected and access network resources.

"StealthWatch can block suspicious network devices by initiating segmentation changes, providing rapid response to identified malicious activity," Hritz said. "ISE can then modify access policies for Cisco routers, switches and wireless LAN controllers embedded with TrustSec technology."

To the Edge and into the Cloud

Branch office security has become increasingly critical as more remote locations access the Internet directly rather than backhauling traffic through the data center. This approach reduces WAN costs, but branch offices lose the inherent threat protection the data center provides.

Cisco Security Everywhere extends enterprise-class security across the WAN to branch locations. Cisco FirePOWER Threat Defense for Cisco integrated services routers protects branch offices by integrating centrally managed next-generation intrusion prevention and advanced malware protection into the network fabric.

Cisco AnyConnect enables secure mobile access by extending threat protection to a wide range of endpoints. Cisco ISE integrates with the Cisco Mobility Services Engine, so IT can create and enforce location policies that define access to data down to a specific room.

Cisco also has advanced its Security Everywhere strategy deeper into the cloud with Cisco Cloud Access Security (CAS). Cisco CAS delivers increased visibility into applications that employees might bring onto the network, detects malicious behavior, and enables policy application and management.

"According to Cisco Cloud Consumption Services trend data, the number of unauthorized cloud applications in use in the enterprise is 15 to 20 times higher than CIOs predicted," said Hritz. "The new Cisco CAS offering allows organizations to address 'shadow IT' and increase visibility and control over data in cloud applications."

Organizations are seizing the opportunities offered by expanding their network boundaries and embracing the Internet of Everything. Cisco's Security Everywhere strategy can help ensure that these opportunities don't come at the cost of compromised systems and data.

"By embedding security into the network, Cisco greatly reduces complexity and risk," Hritz said. "It enables organizations to further expand network access while protecting against constantly evolving threats."

News Briefs

Smartwatches Vulnerable, Study Says

Smartwatches with network and communication functionality represent a new and open frontier for cyberattack, according to a recent study conducted by HP Fortify. The study found that 100 percent of the tested smartwatches contain significant vulnerabilities, including insufficient authentication, lack of encryption and privacy concerns.

HP combined manual testing along with the use of digital tools and HP Fortify on Demand to assess 10 smartwatches and their Android and iOS application components. The company did not disclose which devices it tested, but said it is alerting the vendors.

The main flaws in the majority of smartwatches tested include outmoded transport encryption, poor user authentication and web interfaces that were insecure. Notably, every single device examined lacked a two-factor authentication process — a robust security method that requires users to submit two different types of ID when accessing a particular service.

"Smartwatches have only just started to become a part of our lives, but they deliver a new level of functionality that could potentially open the door to new threats to sensitive information and activities," said Jason Schmitt, general manager, HP Security, Fortify. "As the adoption of smartwatches accelerates, the platform will become vastly more attractive to those who would abuse that access, making it critical that we take precautions when transmitting personal data or connecting smartwatches into corporate networks."

Software Drives Power Grid Modernization

As power grid operators and managers address the growing challenges of stability and reliability in the grid, modern IT solutions are increasingly being leveraged to automate control and maintenance and to more efficiently engage with customers. These new systems are expected to represent a significant portion of smart grid investment over the next decade.

According to a recent report from Navigant Research, the global market for smart grid IT software and services is expected to total $142 billion from 2014 through 2024.

"Platforms like mobile devices and social media are helping to deliver information to utility managers in a way that has never been possible before," says Richelle Elberg, principal research analyst with Navigant Research. "The information and accessibility these new IT systems provide are giving utilities a newfound ability to improve efficiency, reduce their costs, and interact with their customers."

According to the report, utilities are increasingly requiring field and office workers to have access to system data wherever they go. This change is being driven by utilities' desire for heightened productivity and improved workflow management among workers in the field, and it is assisted by the growing presence of broadband networks and the use of smartphones and tablets, all of which are helping the market to expand.

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
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

Software-Defined WAN

SDN principles improve the performance and reliability of branch network links.

The need to connect countless objects, devices, people and applications is fundamentally changing the way workloads move through the network. Cloud computing, mobile access, federated applications and unified communications are among the services that have significantly increased network traffic and intensified connectivity demands.

These demands are particularly acute in organizations with multiple locations and distributed workforces. Remote sites require wide-area network (WAN) connectivity with the performance and reliability to support a full complement of mission-critical services and applications.

Industry analysts say applying the principles of software-defined networking (SDN) to the network edge can bring new levels of reliability and functionality to the WAN. The software-defined WAN (SD-WAN) enables IT organizations to dynamically mix and match connectivity options to optimize traffic, improve application performance and control expenses.

"SD-WAN is a new and transformational way to architect, deploy and operate corporate WANs, as it provides a dramatically simplified way of deploying and managing remote branch office connectivity in a cost-effective manner," Gartner analysts Andrew Lerner and Neil Rickard wrote in their July 2015 technology overview.

Connectivity Choices

SD-WAN allows an organization to blend transport types such as MPLS and broadband to suit their specific needs. While Internet broadband circuits deliver more cost-effective

bandwidth than a service provider's dedicated MPLS connection, MPLS offers more functionality and security, making it ideal for mission-critical and sensitive data.

In a traditional WAN environment, the manual configurations required to differentiate and segment traffic are complex and time-consuming. These configurations need to be updated regularly as application profiles and business needs change, which would require IT to visit each location for every update. As users and organizations demand greater flexibility and agility, and computing continues to shift to mobile and the cloud, the cost and complexity of traditional WAN models are becoming unsustainable.

SD-WAN enables organizations to centrally manage and automate configurations of WAN edge routers. Rather than having a single active network and a backup connection, all connections are active, and traffic routing is automated across a hybrid network that includes public broadband, private MPLS, Internet VPNs and LTE.

Cost Efficiency

SD-WAN reduces costs by making it possible for organizations to rely more upon broadband and less upon more expensive, private MPLS links. SD-WAN is intelligent enough to know when broadband won't provide an adequate connection and reroutes traffic to MPLS on an "as needed" basis. Complex configurations that were previously manual are automated through the SD-WAN application. IT only has to define and prioritize various types of traffic and routing policies instead of constantly reconfiguring devices. Routing is based upon the current state of the network, providing the flexibility to adapt to changing network conditions.

SD-WAN also provides network functions virtualization, which virtualizes all network services. Rather than requiring IT to manage a number of appliances to provide WAN functions, SD-WAN brings these functions to one device where they can be centrally managed and deployed on demand.

SD-WAN appears to be catching on. A recent IHS Infonectics survey of 150 businesses in North America found that 45 percent intend to increase spending on SD-WAN over the next two years.

"Within the data center, raw speed with support for software-defined networking and virtualized workloads are the top requirements for fabrics," said Cliff Grossner, IHS research director. "Meanwhile, outside the data center, SDN-led transformation is taking hold in the WAN optimization market. There's a shift from optimizing application traffic flows over a single point-to-point WAN link to automated and dynamic load balancing of application traffic over multiple link types — MPLS, broadband, Internet, cellular, et cetera."

Better Backup

Cloud and virtualization-specific backup options help overcome the limitations of traditional solutions.

Data backup is arguably the most critical function in IT, but it continues to be a frustrating and problematic process for most organizations. Although backup products and technologies are continually evolving, industry surveys repeatedly reveal that organizations of all sizes are encountering significant backup issues related to cost, complexity and reliability.

Too often, backup technologies and processes have not kept pace with growing data volumes, making it difficult to complete backups within the available window. Increased adoption of server virtualization and cloud-based services have only exacerbated the problem.

"It's a different world for IT managers today, and data backup … is more complex than ever," said Eric Burgener, IDC research director. "Data sizes and types continue to evolve, as does the number of servers and operating systems each company uses. This leads to a host of new challenges IT managers face to make sure they can back up and protect their data and restore operations quickly."

The Game Changer

Backup was a reasonably straightforward affair in the days when applications ran on dedicated servers. Once an application triggered a backup process, most of the server's memory, storage and CPUs were available to the backup application. Server virtualization changed all that by allowing multiple virtual machines (VMs) to run on a single piece of hardware. Resource contention becomes a serious issue when an organization is simultaneously backing up physical, virtual and cloud environments featuring consolidated workloads and extreme data redundancy. If a hypervisor runs out of memory, it can cause a server crash that can bring down multiple applications.

At the same time, there is more data to be backed up and backups need to be completed more frequently to meet recovery point objectives. The problem becomes exacerbated as the environment scales to hundreds or thousands of VMs sharing a common resource pool. Agent-based backup solutions place a significant burden on host servers and make it difficult, if not impossible, to complete backups within the available window.

Virtualization-aware, host-level backup is far superior to agent-based solutions, but it presents a separate set of issues. These solutions typically use snapshots to create image-level backups then track block-level modifications. Challenges arise when VMs are moved from one server to another — a host may be running a different set of VMs than it was when the last backup was made. And while an image-level backup makes it easier to recover an entire VM, it requires at least a two-step process for file-level recovery.

In this scenario, backup is easy but recovery can be difficult. File-level recovery allows administrators to restore individual files in minutes without the time-consuming process of extracting the full VM image to a local drive. Organizations need this capability to support mission-critical applications running on VMs.

Purpose-Built Solutions

Best-of-breed backup solutions for virtualized environments offer file-level restore as well as replication rollback capabilities, protecting VMs from both hardware failure and software corruption. IT can recover individual items from any virtualized application, on any operating system, without additional backups, agents or software tools.

Virtualization-specific backup and replication gives organizations greater confidence to virtualize enterprise applications such as CRM, ERP and email systems. The ability to restore an entire VM from a backup file in minutes means that users remain productive while IT troubleshoots the issue.

Virtualization-specific solutions with synthetic backup capabilities eliminate the need to run resource-intensive full backups. After an initial full backup, only changes are stored, and a synthetically compiled full backup is available for fast restore at any time. This technique reduces backup time and bandwidth utilization. Incremental changes are tracked to allow for rollback in case of software failure or corruption.

De-duplication further improves backup efficiency. When backing up multiple VMs, de-duplication software stores only one instance of similar blocks, saving time and storage space. This becomes an important issue when backing up VMs created from a single template, or VMs with significant free space on their logical drives.

With VM replication, copies of mission-critical VMs are mirrored to a spare server and kept in the ready-to-start native format. This capability enables cost-effective disaster recovery for mission-critical applications and data. Should a failure occur, IT can run a VM directly from a compressed and de-duplicated backup file on regular backup storage, either in production or an isolated virtual lab.

The Cloud Option

Under certain conditions, shifting data backup to a cloud provider can be a good option. Cloud-based backup requires no capital investment for equipment and makes backup an operational cost. Software encrypts data for security purposes and automatically backs it up to remote servers. The service provider maintains and monitors the data backup plan, and because data is saved at a different location, it's always accessible.

Restoring large amounts of data from the cloud can be time-consuming, however. Hybrid solutions help avert such performance issues by keeping primary storage onsite on disks or NAS appliances and moving secondary storage and data backup to the cloud.

Although data backup is critical to any organization, the process has become painful for most IT departments. Virtualization and cloud services have fundamentally changed the process, making it nearly impossible to manage with traditional backup solutions. Virtualization-specific backup solutions with incorporated de-duplication and VM replication capabilities have become the gold standard — but there are other good options, depending on the organization's specific requirements. For a smaller organization with a modest data footprint, a hybrid cloud backup strategy can deliver compelling economic and management benefits.

Cloud Backup Requires Vigilance

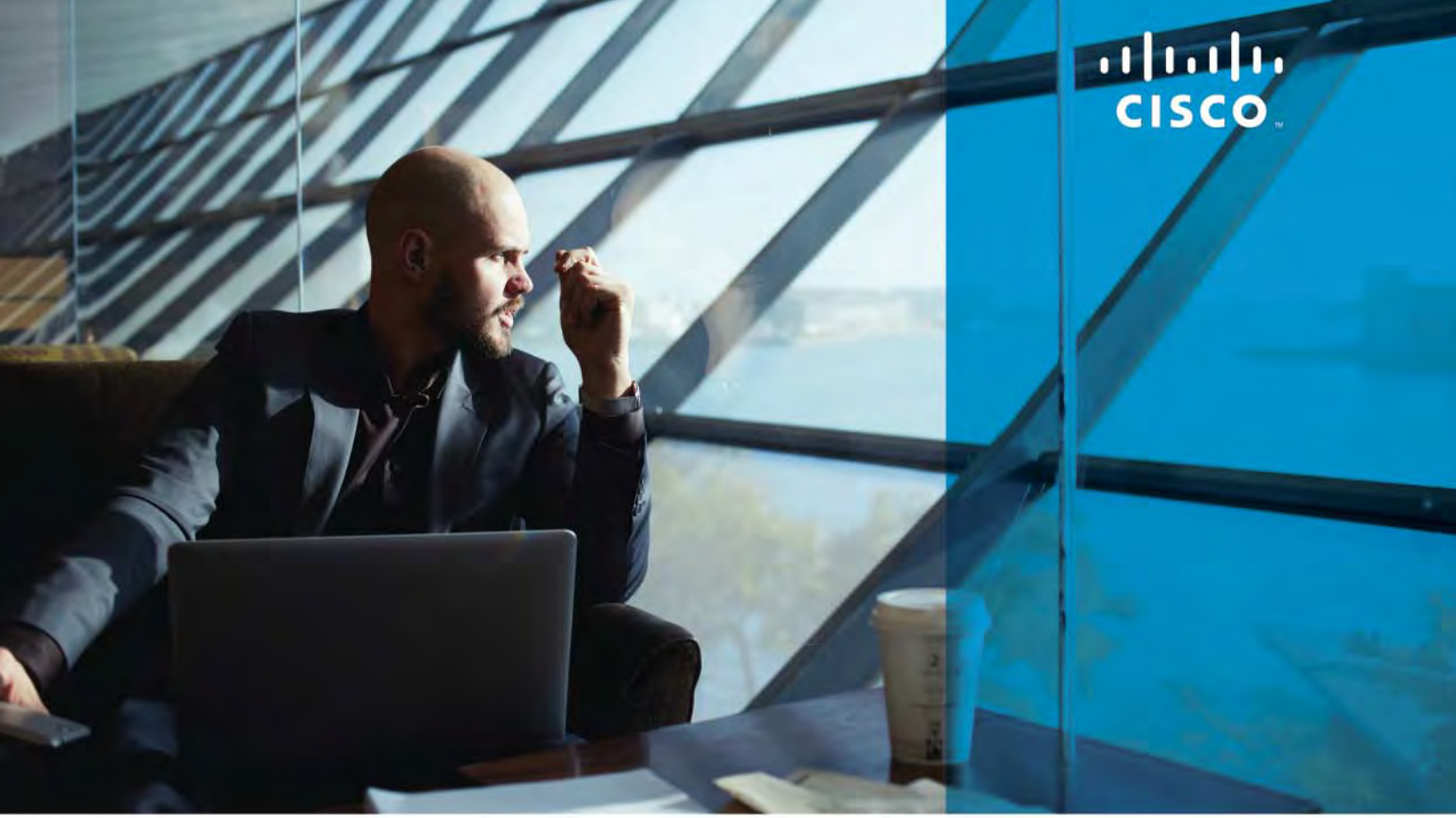
For many organizations, cloud backup is a simple, powerful and affordable solution that solves a significant problem and delivers peace of mind. However, the SANS Institute warns that the security risks involved in transmitting important data across the Internet to an off-site server can't be ignored.

Organizations need to keep security close to their data as it traverses cloud systems by controlling permissions and access to the data as well as encrypting it, according to a report from the cooperative research and education organization.

In a recent survey, the SANS Institute found that reliance on cloud services continues to increase, with organizations moving a broad range of applications and operations to the cloud. Eighty percent of respondents either have or plan to have a cloud service implementation within the next 12 months.

However, 58 percent said they lack visibility in cloud providers' operations and are unprepared to respond in the event of a breach of cloud-based data.

"Moving collaboration tools, email tools, managed services and backup and recovery to the cloud solves some problems for organizations, but with that increased cloud functionality comes increased security risk," says SANS analyst and survey author Dave Shackleford. "Organizations need integrated monitoring capabilities across their hybrid environments and partnerships with public cloud providers for full-spectrum visibility and response."



Security matters more than ever. That's why we're putting Security Everywhere.

Traditional approaches to network security were designed for a single purpose: to protect resources inside the network from threats and malware coming from outside the network. Today's businesses must consider smartphones, tablets and consumerization of IT, combined with telecommuters, contractors, partners and business-critical services hosted in the cloud. Security is more important than ever — and far more complex.

Through our Security Everywhere strategy, Cisco is acknowledging this new threat landscape and addressing it in a far more comprehensive and integrated manner than ever before. The value of Cisco architecture is its emphasis on embedding security spanning the extended network — from the data center to the cloud to every endpoint — closing gaps across the attack continuum and significantly reducing time to detection and remediation.

Contact your ProSys representative for a more in-depth discussion of the product, solution and services enhancements comprising a Security Everywhere approach, and how they can enhance your protection against a growing array of security threats.

www.prosysis.com
888-337-2626

PROSYS
A PIVOT COMPANY