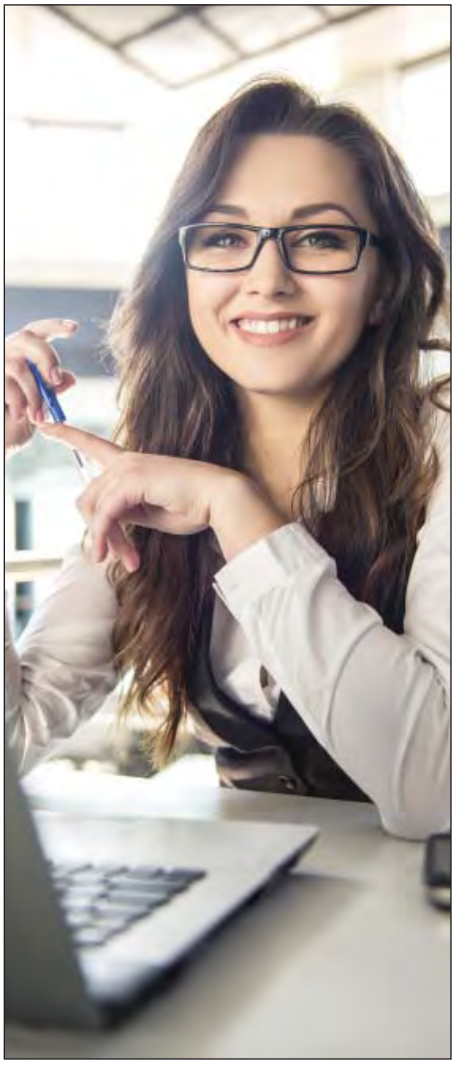
Tech Outlook

March 2016

PROSYS
A PIVOT COMPANY



Streamlining App Delivery

Citrix NetScaler eliminates IT complexity and improves performance, scalability and security.

In the very recent past, workplace technology consisted entirely of corporate-owned assets fully controlled by IT. Key tasks were performed on locked-down hardware running desktop-bound software installed on a local server and accessed across the local network.

Today, such an arrangement seems about as retro as Dictaphones and secretarial pools.

"The mobile-cloud era has introduced a diversity of applications, data and devices into the workplace," said Michael Hritz, Business Development Manager, ProSys. "Employees commonly use both company and personal devices to access a variety of applications and services on either side of the firewall — and they expect that these apps will be instantly available on demand."

The need to efficiently deliver applications across all types of networks, to any device at any location and at any time of day or night creates significant complexities for IT organizations. Servers must be able to handle sudden or unpredictable changes in demand with no lag in application performance. The traditional data center practice of server overprovisioning is too costly and slow.

Citrix NetScaler application delivery controllers (ADCs) relieve this burden by performing a broad range of functions to enhance the performance, scalability and security of applications. Designed with an eye toward managing Web apps and user traffic to those apps, NetScaler ensures resources can

continued on page 2

TECH OUTLOOK

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

continued from page 1

be dynamically tiered, provisioned and accessed across dispersed and mobile groups of users.

"NetScaler makes applications run five times better, reduces Web application ownership costs and makes sure that applications are always available," said Hritz. "It is deployed in thousands of networks around the globe to optimize, secure and control the delivery of all enterprise and cloud services and enhance the computing experience for every user, including mobile clients."

Loads of Functionality

Deployed in front of web and database servers, NetScaler combines high-speed load balancing and content switching, data compression, content caching, SSL acceleration, network optimization, application visibility and application security on a single, comprehensive platform.

Load balancing is one of the key functions of any ADC, allowing IT to balance application workloads across a cluster of servers to optimize resource use, maximize throughput, minimize response time and avoid overload of any single server. In basic ADCs, simple algorithms are employed to direct traffic based upon attributes such as the HTTP header.

However, NetScaler employs the industry's broadest array of load balancing technologies for more precise routing. NetScaler considers attributes such as SSL session ID, Uniform Resource Identifier, the client location, the type of content requested and an array of payload value information to make balancing decisions.

Beyond load balancing, NetScaler employs other tools such as resource monitoring and analytics to increase application availability. NetScaler continuously monitors the availability and health of server hardware, back-end databases and applications. Additionally, NetScaler checks network links, operating systems and even individual application elements to ensure traffic is routed only to fully functional servers, thus preventing bottlenecks and session redirects.

Security Boost

NetScaler also plays an instrumental role in an organization's security posture.

While mobile and cloud technologies deliver indisputable productivity benefits, they also raise security and privacy concerns by creating new network attack vectors. With the erosion of traditional network perimeters, many organizations have employed a variety of specialized gateways for accessing cloud apps and services. The result often is a fragmented security environment characterized by multiple URLs, spiraling complexity, increased costs and poor user experiences.

"NetScaler makes applications run five times better, reduces Web application ownership costs and makes sure that applications are always available."

NetScaler ADCs with Unified Gateway features consolidate mobile and cloud access methods and simplify remote access to applications and services deployed in the data center or the cloud. With one URL, NetScaler becomes the single secure access point for all web and mobile apps and services. NetScaler is also widely deployed as an authentication gateway for external users seeking access to network resources. Its ability to process encrypted SSL/TLS traffic allows it to securely validate users' identities and offload these compute-intensive tasks from back-end servers.

NetScaler also incorporates numerous application-layer protections, including a full-featured application firewall, data loss protection, and countermeasures for thwarting denial-of-service (DoS) and other Layer 7 attacks.

"With an extensive portfolio of essential security capabilities, NetScaler minimizes the need to invest in a large number of expensive standalone solutions," said Hritz. "It enables organizations to improve their security footprint with their existing infrastructure."

Stretching the Budget

That "more with less" capacity is particularly important given the current budgetary constraints in most IT organizations. In a recent Total Economic Impact study of NetScaler, analysts with Forrester Consulting cited the multipurpose nature of the solution as a major factor in helping organizations reduce costs, automate tasks and improve application reliability.

For the study, Forrester created a composite organization based upon interviews with four companies using NetScaler. This composite organization realized nearly $500,000 in annual savings for network devices that could be retired, replaced or avoided. Because fewer devices were needed, the organization also saved $120,000 per year in maintenance, support and licensing costs. Most important, IT tasks were streamlined and applications became more reliable.

"Most organizations implement ADCs for load balancing, but NetScaler can do so much more," said Hritz. "At a time when mobile and cloud technologies are introducing complexity into the IT environment, NetScaler delivers simplicity by performing so many key functions. With improved application performance, reduced downtime, increased automation and better security, it is one of those rare solutions that really does let you do more with less."

News Briefs

Big Data Projects Bring Good Results

Big data initiatives are delivering generally positive early results for the companies that have launched projects, according to a survey from CompTIA, the IT industry association. The organization reports that 72 percent of companies that have launched some form of big data initiative say that their results have exceeded expectations.

While early returns are encouraging, the study also reveals that much more work must be done to harness and make use of data.

"The amount of data crossing the wires and airwaves is mind-boggling," said Seth Robinson, senior director, technology analysis, CompTIA. "So while individual pieces of a holistic data solution may be improving, these individual pieces are not yet integrated in a way that drives ideal results."

Approximately three-quarters of organizations surveyed by CompTIA say that their business would be stronger if they could harness all of their data. Additionally, 75 percent of companies said they should be more aware of data privacy, while 73 percent said they need better real-time analysis.

Organizations also express a willingness to work with third parties for help with their data initiatives. Over one-third of companies currently work with an IT firm for their data needs, though these engagements tend to be somewhat simplistic (data storage and data backup, for example). But as companies become more aggressive with their data initiatives, IT firms may find opportunities to offer comprehensive services around data.

Spreading Flu in the Workplace

Although American workers are well aware of the impact of the flu on workplace productivity, more than half of those responding to a recent survey admit they have gone to work with the flu. According to the annual Staples survey, 58 percent of employees go to work sick because they feel there is too much going on at work to take a sick day — an uptick from 30 percent in 2012.

A high percentage of survey respondents indicated a strong knowledge of flu protection techniques, and 88 percent said they have encouraged sick colleagues to go home. Yet, they don't practice what they preach.

Half of workers feel the pressure to be at work or "tough it out," and 25 percent don't feel confident that someone else can handle their work when they're out sick. It is an even bigger issue at the management level, with 30 percent of business decision-makers indicating their boss expects them to come to work if they have the flu. Additionally, 39 percent said they think going to work while sick shows that they have extra initiative.

"It's encouraging to see that employees have a strong understanding of flu risks and prevention, but there's still work to be done," said Dr. Charles Gerba, a professor of microbiology and environmental sciences at the University of Arizona who studies the transmission of pathogens through the environment. "The flu wreaks havoc on U.S. employees and in turn on businesses every year. Simple measures such as cleaning, sanitizing and limiting exposure can make a huge difference."

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

Rethinking Patch Management

Continuous software updates are becoming the norm as security threats continue to multiply, but there are risks to this approach.

Historically, software vendors released security patches on a monthly or quarterly basis — Microsoft's "patch Tuesday," on the second Tuesday of every month, is probably the most famous example. However, the ever-growing number of IT security threats has led to a corresponding increase in the number and frequency of patches issued by vendors. These patches must be applied to systems promptly to protect against cyberattack. This is particularly true given the rise of so-called zero-day exploits that take advantage of a security vulnerability the same day the vulnerability becomes generally known.

Consumers are growing accustomed to frequent software updates on their mobile devices, and with Windows 10 Microsoft is abandoning "patch Tuesday" in favor of releasing updates as soon as they become available. The faster patches are released and applied, the more likely the system will be protected against emerging threats. However, this scenario creates a number of other risks for business.

When a patch is rolled out quickly, there's an increased chance that it will introduce bugs, create incompatibilities or have other unintended consequences. Microsoft has released buggy patches in the past, and recently withdrew a cumulative patch for Windows 10 after users reported system crashes.

Generally, IT departments prefer a more conservative approach to patch management, thoroughly testing each update to ensure that it doesn't have bugs or conflict with legacy software. Approved patches are then rolled out to users in a controlled manner that preserves network bandwidth and minimizes productivity drains.

That said, frequent, automated patches can be a boon to harried system administrators by relieving some of the patch management burden and ensuring that systems are better protected. The trick is to strike the appropriate balance between security and productivity.

Develop a three-prong patch strategy. Continuous updates with no user interaction may be appropriate for low-priority applications, while continuous updates controlled by IT might be better suited for end-user devices and productivity apps. Mission-critical systems will still require a traditional patch management approach with testing, val-

idation and change management protocols.

Prioritize patches. IT teams should adopt a risk-based approach to patch management. For example, a zero-day attack on a mission-critical or customer-facing application should take priority over scheduled releases of patches for less-exposed systems.

Take inventory. The key to patch management is effective software management, but few organizations have an accurate inventory of what is installed on each piece of equipment. Automated systems can gather information about which versions of what software are running and which patches and services packs have been applied. An accurate inventory streamlines patch management and helps administrators identify which patches need to be installed.

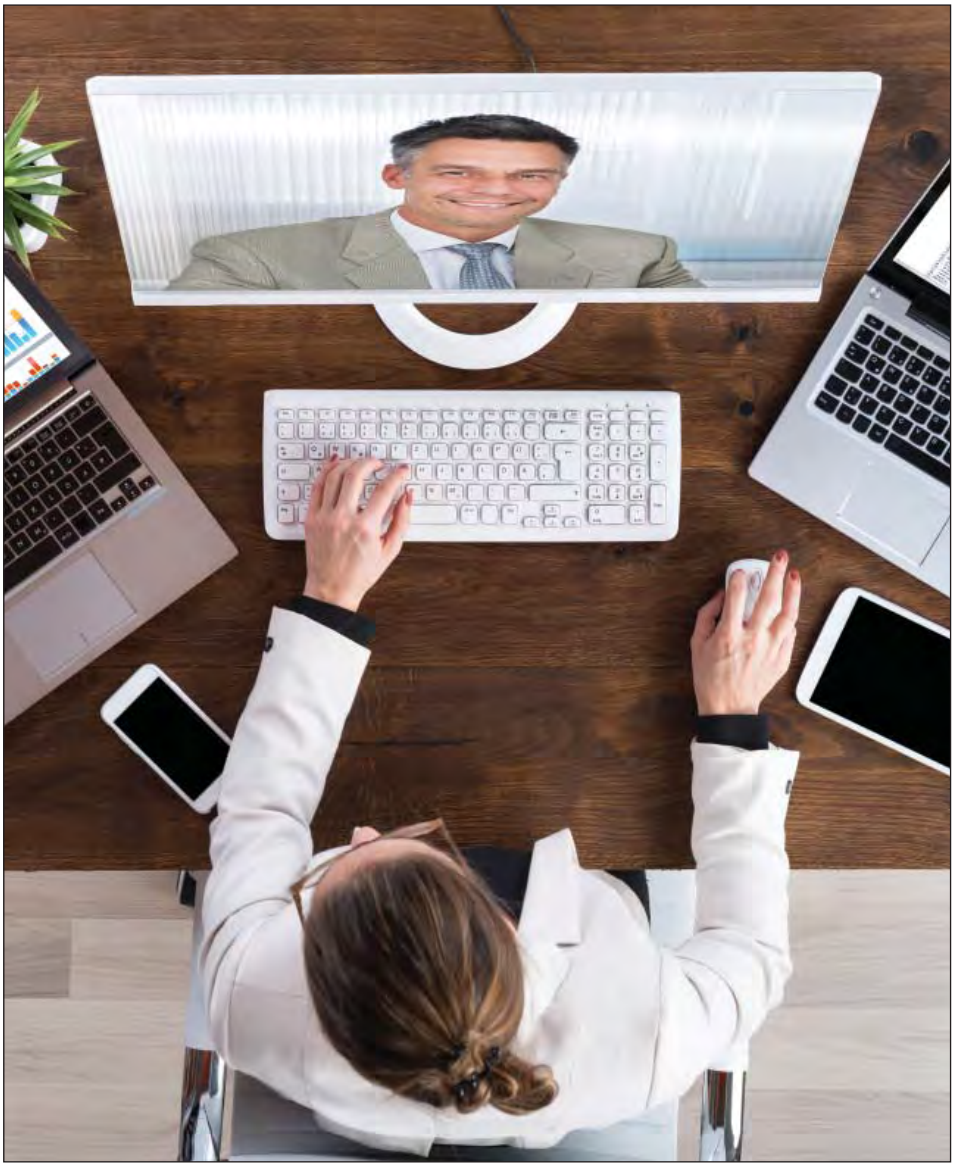
Standardize systems as much as possible. Most companies have more than one operating system to manage, increasing the number of patches to be applied. Reducing the number of platforms eases the patch management burden and helps reduce the possibility that applied patches will adversely affect other systems.

The one strategy that definitely won't work is to avoid patching systems altogether. Most cybercriminals rely upon decades-old techniques exploiting vulnerabilities that have been open for years. Verizon's 2015 Data Breach Investigations Report noted that 99.9 percent of cyberattacks exploited vulnerabilities that had been reported more than a year earlier, including some that could be traced to 2007. These vulnerabilities remain open even though patches are available to fix them.

Falling behind on patch management is more than just a security risk — it can have a negative impact on system performance and unnecessarily increase operational costs. Patching is going to continue to be a job requirement for system administrators, but with the right strategy it doesn't have to be a full-time job.

Automating Unified Communication

Optimizing voice and video traffic with network programmability.



It's easy to understand the value of a single, computer-based system that unifies all communication options one might choose — phone, text, video, document sharing and more. By integrating all these applications, unified communication (UC) platforms deliver a multitude of business benefits including improved employee collaboration, productivity and customer service.

However, UC also places considerable demands on IP networks. Ensuring an acceptable user experience typically requires the implementation of significant Quality of Service (QoS) measures to ensure bandwidth availability and minimize latency, jitter and packet loss.

"Networks are becoming increasingly congested due to the growing consumption of media-rich applications such as video and UC," said Kevin Riley, chief technology officer of Sonus Networks. "Historically, network operators have overprovisioned their networks to handle this congestion, which has resulted in inefficient network monetization. This model is no longer economically feasible. A solution is required which can deliver predictable behavior … via intelligent network control and application-aware policies."

Software-defined networking (SDN) technologies show promise for delivering just such a solution, and ensuring critical communication applications have the network resources they need for reliable performance. SDN makes the network programmable, with applications dictating the behavior of switches and routers, shaping traffic, and controlling the flow of data packets.

Quality Challenges

Because most IP networks were designed for "best effort" delivery, the data packets that traverse them are frequently subjected to traffic and routing problems that delay their arrival at their destination. Packet loss, latency and jitter are all issues related to the speed and order of delivery of data packets. As the name implies, packet loss occurs when packets do not reach their destination at all, while latency and jitter occur when packets arrive out of order or at uneven intervals that cannot be offset by buffering.

Users seldom notice data traffic delays unless they are significant. However, the problems are far more pronounced for UC traffic. The human ear is able to pick up even the slightest delays in a voice call, and such issues are even more noticeable in a videoconference.

IT engineers use a variety of QoS services to avoid such issues and ensure acceptable voice and video performance. However, it is a challenging process — particularly since UC traffic is generally encrypted for security and confidentiality reasons. With insufficient visibility into this traffic, network administrators

must resort to complex and error-prone manual networking provisioning to enable QoS, path selection and bandwidth reservations.

For example, all voice and video packets must have appropriate header markings that identify them as high-priority network traffic. All switches and routers along the path must be manually configured to recognize those markings. Additionally, engineers must populate network devices with tables that map these header markings to precise Class of Service (CoS) values for differentiating payloads. However, it is difficult to extend the process beyond internal networks. Service providers generally have their own QoS services and don't trust header markings coming from beyond their "trust boundaries."

'Configuration Drift'

Ensuring that UC works reliably over a Wi-Fi connection adds another layer of complexity. As the mobile workforce continues to grow, providing voice, video and collaboration across the wireless LAN has become a business imperative. However, establishing QoS for UC traffic moving over a WLAN requires using a different set of CoS tags and a different traffic-prioritization standard than in wired networks.

This all adds up to an increasingly unstable arrangement. Given the complex interplay between devices across wired and wireless networks, configuration changes often have a domino effect. In a hardware-centric network, tiers of switches and routers implement diverse protocols to connect devices using proprietary interfaces. Any change to the network requires multiple updates to protocol-based mechanisms using device-level management tools.

Changes can take days or weeks, making it difficult to maintain a consistent set of QoS settings. Over time continual changes can cause what's known as "configuration drift" — a state of inconsistent configuration that creates management problems and can lead to serious availability issues.

The non-profit International Multimedia Telecommunications Consortium (IMTC) says these issues have a negative impact on Quality of Experience (QoE), which is a measure of a customer's experiences with UC services. According to the IMTC, information from UC systems suggests that up to 80 percent of QoE problems are actually caused by issues with the underlying network.

Introducing Automation

A number of industry groups, including the IMTC, the Open Networking Foundation and the Unified Communications Interoperability Forum, believe SDN is the best route to resolving UC quality issues. Over the past year, these groups have developed several proposals for using SDN to dynamically configure network infrastructure to meet UC traffic requirements.

SDN doesn't alter the basic network infrastructure — it simply uses software to eliminate manual configuration tasks. SDN moves the "control plane" of the network away from each individual device on the network to a controller that works with all the devices, including both virtual and physical devices.

In the UCI Forum's specification, SDN makes it possible to dynamically set several key QoS settings for UC traffic, including marking voice and video packet headers, adjusting bandwidth associated with specific CoS settings, and routing along a path that is best able to meet performance requirements — rather than along the "default" least-cost path.

"This innovative approach removes the expensive and error-prone manual administration of deploying QoS, thereby eliminating misconfiguration, configuration drift and increased cost of operations," the UCI Forum said in announcing its specification. "All an operator has to do is specify a set of policies for voice, video and web conferencing and the UC systems will automatically program the network."

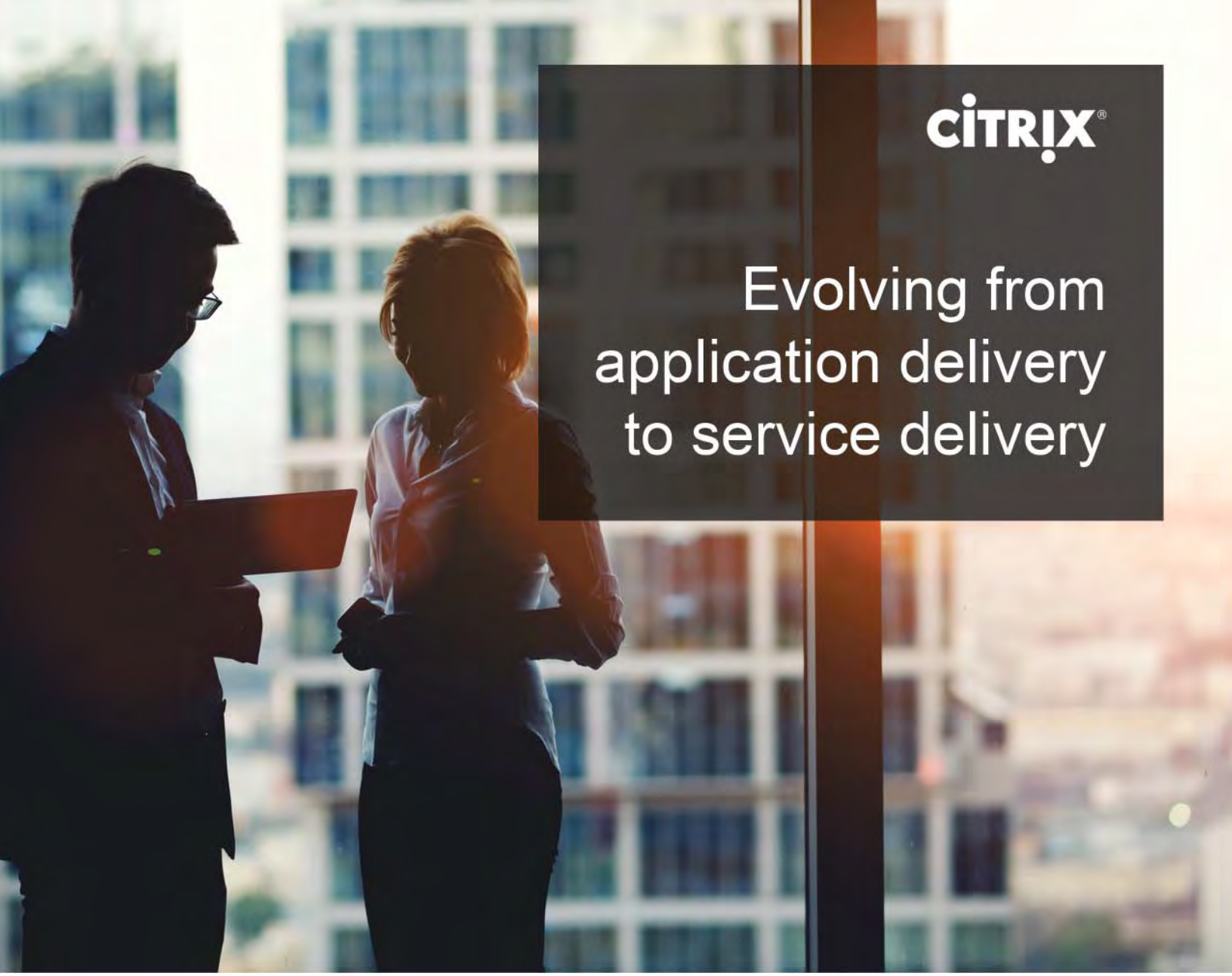
UC Users Want Better Tools and Training

While end-users overwhelming agree that unified communications (UC) platforms enhance their job performance, most say their UC tools have plenty of room for improvement. In a recent study of UC users conducted by International Data Group, more than a third said their tools are merely "satisfactory" or even "poor."

Nevertheless, respondents were overwhelming enthusiastic about the end results. The survey found that 97 percent reported improved collaboration, and 93 percent reported increased productivity. Additionally, 88 percent reported improved problem resolution and 81 percent reported fast decision-making.

Respondents reported that the two UC tools having the most direct positive impact on productivity are presence detection and multichannel contact centers. Presence detection allows users to see who is available and identifies the best way to reach them, while multichannel contact centers help decrease the average time it takes to resolve customer issues.

While respondents were clear about the benefits of integrating UC into their daily work, 24 percent indicated they had not received sufficient training so they could maximize the value of the UC tools available to them. Proper training helps workers increase the use of UC features and improve productivity.



The role of IT is shifting away from building applications and operating infrastructure, towards orchestrating a variety of both internal and external apps and services and delivering them to business users. But traditional application delivery products and technologies can't fully support these new roles.

Citrix NetScaler SDX™ application delivery controllers support the transition to a service delivery model by making applications run five times better, reducing application ownership costs, and ensuring application availability. NetScaler not only maximizes the performance and availability of all applications and data, it also provides secure remote access to any application from any device type.

Contact ProSys to learn how Citrix NetScaler can improve your business computing infrastructure.

PROSYS
A PIVOT COMPANY

www.prosysis.com
888-337-2626