VERTEKS CONNECTION

VOLUME 9 NUMBER 2

VERTEKS
VOICE & DATA
NETWORKS

Ready to Grow

Verteks deploys ShoreTel UC with ShoreTel Enterprise Contact Center to provide Triage Management with a strong platform for continued growth.

Wind or hail damage is a stressful situation for any homeowner, and finding a reputable and qualified roofing contractor only adds to the anxiety. Triage Management Services helps to relieve that anxiety.

The Jacksonville, Fla.-based firm has built a network of pre-screened roofing contractors who specialize in the repair of wind and hail damage. Operating under the name First Choice Repair, the company also streamlines the estimating process and insurance paperwork for homeowners, and backs the contractor's five-year warranty on workmanship with its own guarantee.

Triage has been growing rapidly, and needed a phone system and contact center solution that would better support its business requirements. The company called on Verteks Consulting to replace an aging NEC system with a state-of-the-art ShoreTel solution.

"We had an older system that just could not accommodate our growth," said Karen Spiegelberg, Manager of Business Applications, Triage Management Services. "We needed something a

continued on page 2

VERTEKS CONNECTION

PRESORTED
FIRST CLASS
US Postage
PAID
Tulsa, OK
Permit #2146

little more robust and easier to work with. We started looking around at various companies, and consulted with a few. Then we came across Verteks and decided to give them a shot.

"They were very accommodating from the get-go. They came to visit us, sat down and listened to our needs, and came up with a solution. They were fantastic to work with in getting us what we needed and not trying to oversell us on a system that we weren't quite ready for."

Key Component

The contact center is an important part of Triage Management's business — not only for customer support but for generating revenue. The ShoreTel Unified Communications (UC) Solution with ShoreTel Enterprise Contact Center has call management features that enable the firm's small staff to efficiently handle growing call volumes.

"It's very key to us," Spiegelberg said. "Right now, we're using it to manage inbound calls and route them appropriately. It helps us keep those lines open, which keeps revenue coming in. We're also excited about being able to use the outbound dialer in the near future."

The company has about 65 agents taking calls, as well as managers and other personnel who utilize the system. The ShoreTel Enterprise Contact Center solution gives Triage the flexibility to adapt to meet changing business requirements.

"We really like having the ability to dynamically create groups," Spiegelberg said. "We're not a large company and our agents tend to cover multiple groups at one time. That's the flexibility we were looking for, and that's what we found with the system."

Triage is also taking advantage of the management and reporting tools that are built into the ShoreTel system to improve its operations.

"Our managers love it," said Spiegelberg. "They can see if one group is starting to get heavy traffic, and if they need to ramp up we can put more people in that group quickly. They can quickly shift people around in responsibilities and priority of how they want calls handled. It has definitely helped them better manage their staff."

All the Right Tools

Verteks took the time to learn about Triage Management's contact center operations and design a solution that would meet the company's needs now and in the future. ShoreTel Enterprise Contact Center has the ability to support multiple communications channels, such as online chat, in addition to phone calls. It can also expand along with the business.

"We're definitely looking at online chat — that's big to us. We're excited to have those extra tools available," Spiegelberg said. "And we're already talking about adding hardware and additional licenses. Verteks has been very helpful in planning all of that. We met with them recently and started laying the groundwork for the next phase of this project."

ShoreTel UC serves as the platform for Triage Management's corporate communications. End-users like the capabilities of the ShoreTel UC solution, which offers many features that simply weren't available on the old NEC system.

"It was a little intimidating to the folks when we first made the cutover," said Spiegelberg. "There was a lot to learn, and we were asking them to take on new technology and still maintain productivity. But they've had it now for a year and half. I think if we threatened to take it away, we'd have mutiny on our hands. A lot of our folks don't even dial anymore — they use the ShoreTel Communicator to dial the phone. They really do love the flexibility it gives them."

A True Partnership

The Verteks team handled the ShoreTel implementation from end to end, doing a lot of work upfront to set up the system according to Triage Management's requirements. Verteks was also on hand to ensure a smooth cutover from the old PBX to the new ShoreTel system.

"The disruption to the business was very minimal because Verteks took on all the initial coding. We sat down, mapped out what we wanted and they coded it," Spiegelberg said. "From there it was a case of disconnecting the old system and getting the new system in place. They had engineers onsite during the cutover to help us out."

The ShoreTel system is very reliable — Triage has experienced only minimal downtime due to factors external to the system. The system is also easy to administer and boasts a very low total cost of ownership (TCO). Should a problem arise, Verteks is there to provide ongoing support.

"They are very quick to respond to any of our needs," said Spiegelberg. "I joke with Don [Gulling, President of Verteks] because I have him on speed dial. And Don recorded my name for me on the phone system, so if you call you hear his voice announce my name. I tell people that's my assistant."

All joking aside, Spiegelberg says Verteks has played a key role in giving Triage Management the communications tools it needs to support its ongoing growth.

"Verteks is great to work with," she said. "They are more than just a vendor — they are a partner in helping us grow our business."

News Briefs

Tablet Apps to Surpass Smartphone Apps

Smartphone apps reign supreme right now, but ABI Research expects tablet apps to catch up and then surpass them as the combined mobile app revenue base nearly quadruples.

Tablet apps will generate $8.8 billion in revenue in 2013, compared to the $16.4 billion expected from smartphone apps, according to the latest forecasts from the research firm. However, tablet apps will steadily increase their share of the market over the coming years. Tablet app revenues will nearly match smartphone app revenues in 2017 and surpass them in 2018, when the combined revenue base will reach $92 billion.

"The dynamic is quite straightforward," said senior analyst Aapo Markkanen. "The larger screen makes apps and content look and feel better, so there are more lucrative opportunities."

Customer Experience a Top Priority

Ninety-seven percent of executives agree that delivering a great customer experience is critical to business advantage and results. Respondents to a recent global survey by Oracle further estimate that the average potential revenue loss for not offering a positive, consistent and brand-relevant customer experience is 20 percent of annual revenue.

Ninety-three percent of executives say that improving the customer experience is one of their organization's top three priorities in the next two years. However, many organizations are stuck in an execution chasm: 37 percent are just getting started with a formal customer experience initiative, and only 20 percent consider the state of their customer experience initiative to be advanced.

Verteks Connection

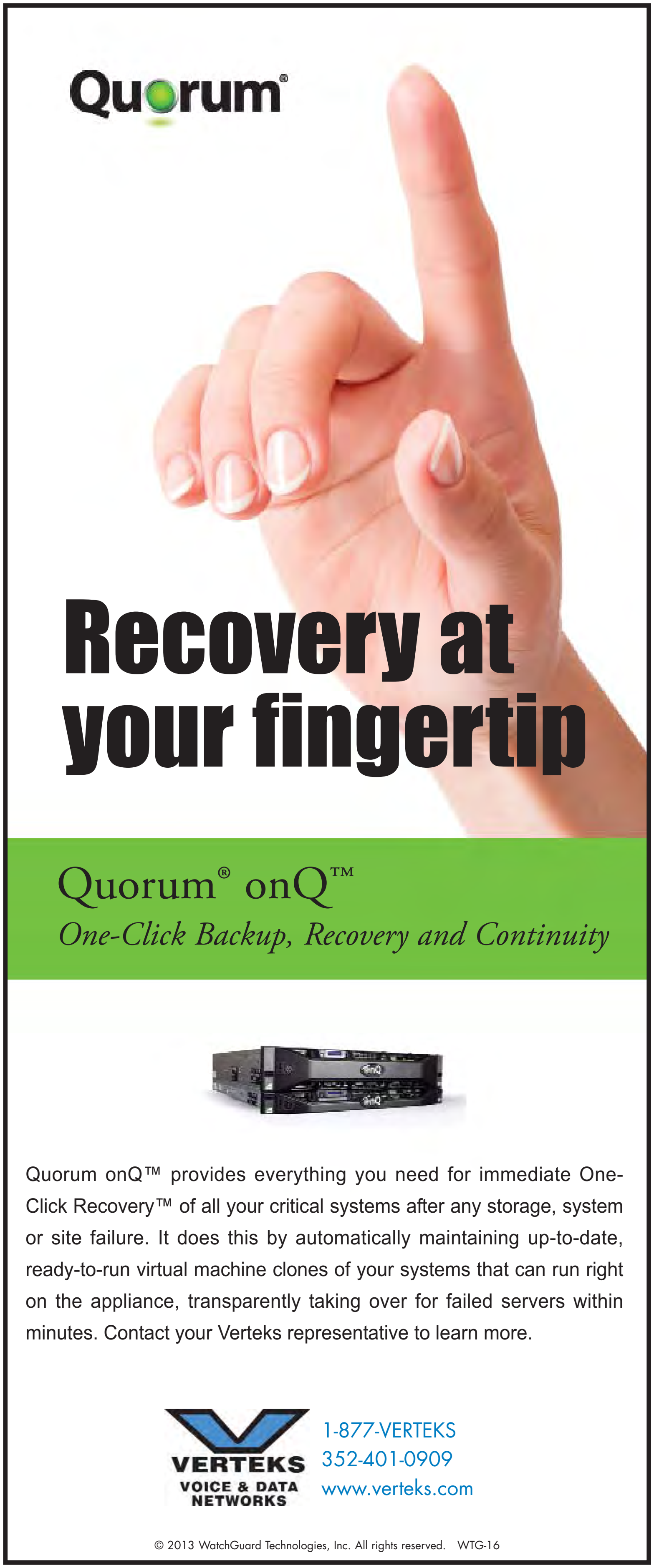
Copyright © 2013 CMS Special Interest Publications. All rights reserved.

Editorial Correspondence:
7360 East 38th Street,
Tulsa, OK 74145
800.726.7667 • Fax 918.270.7134

Change of Address: Send corrected address label to the above address.

Some parts of this publication may be reprinted or reproduced in nonprofit or internal-use publications with advance written permission.

Printed in the U.S.A. Product names may be trademarks of their respective companies.



Quorum®
Recovery at your fingertip
Quorum® onQ™
One-Click Backup, Recovery and Continuity
onQ
onQ
VERTEKS
VOICE & DATA NETWORKS

Quorum onQ™ provides everything you need for immediate One-Click Recovery™ of all your critical systems after any storage, system or site failure. It does this by automatically maintaining up-to-date, ready-to-run virtual machine clones of your systems that can run right on the appliance, transparently taking over for failed servers within minutes. Contact your Verteks representative to learn more.

1-877-VERTEKS
352-401-0909
www.verteks.com

© 2013 WatchGuard Technologies, Inc. All rights reserved. WTG-16

Print, Copy, Scan ... HACK?

Unprotected MFDs open doors for hackers and put sensitive data at risk.

As businesses, institutions and government entities discover the significant benefits delivered by multifunction devices (MFDs), the combination printer/copier/scanner units are gaining an increasing role in the office.

Like most technology in the workplace, copiers and MFDs have evolved to include many new features, such as the ability to wirelessly communicate with computers and smartphones and to fax and email documents through network connections. They also offer economies of scale by serving an office full of users with one machine where previously numerous devices were needed.

The same advances that have given these smart devices so much power have also introduced a host of potential security issues.

No longer are they the comparatively simple devices that required little more than a secure location and controlled access to printer and fax queues. The printers and copiers of the past were immune to the threats of malware or cyberattacks faced by computers, servers and related equipment.

In many cases, the perception of these devices as “safe” has remained stagnant as the capability and complexity of MFDs has increased significantly. Today’s MFDs are built around powerful computing systems loaded with more complex applications than ever and offering connectivity through multiple access points. As such, networked MFDs can no longer be treated like dumb peripherals.

“Over the past decade, greater intelligence has been built into (most) enterprise and consumer equipment … (an MFD) may now contain a fully functional operating system and a computer with processing power dwarfing that of an older desktop computer,” wrote the Washington University School of Medicine in its guide for information security.

The State of Security

While there has been little indication of printer-based attacks spreading across large networks, at least one recent intrusion went a long way toward opening the eyes of IT departments to the importance of identifying and applying security controls consistently across an entire organization. In 2011, a massive breach of Sony’s PlayStation Network led to 77 million accounts being hacked and resulted in millions of dollars of lost revenue for Sony. A similar attack is possible through an MFD if its physical and electronic access points aren’t securely controlled and protected.

In 2010, the CBS news story “Digital Photocopiers Loaded with Secrets” highlighted the potential risk of critical information being stolen from cached data stored on the hard drives of printers and photocopiers. Higher education institutions and government entities have responded with strict guidelines for establishing security controls on MFDs, and most manufacturers now offer data security kits and services to meet hardened industry standards.

Among the most detailed is the Security Technical Implementation Guide the Defense Information Systems Agency developed for the Department of Defense, which “provides the technical security policies, requirements and implementation details for applying security concepts to commercial-off-the-shelf hardware peripheral devices.” The document devotes a complete section to MFDs.

The guide advises, “If an attacker gains network access to one of these devices, a wide range of exploits may be possible. If an attacker gains physical access to a device, the programming of the device can be compromised and the potentially sensitive data stored on the hard disk can be recovered.”

‘Is There Really a Threat?’

Even with these warnings and guidelines, many businesses have been lax about MFD security. Instead of patching and hardening MFDs, IT departments often overlook the devices from a risk management perspective.

A survey commissioned by Xerox and McAfee last year found that some companies don’t take even simple steps to lessen the risk. The survey reported that only 13 percent of employees say they are prompted to enter a password on MFDs before releasing a job they’ve printed or accessing the ability to copy.

There are nearly 30 million printers and MFDs in offices and homes throughout the U.S. and Western Europe, according to an InfoTrends survey of the market in 2010. Considering most of those devices are connected to a network, and the growth in numbers of devices was running from 4 percent to more than 5 percent a year at that time, the opportunity to exploit MFD weaknesses must be increasingly attractive to potential attackers. As PCs and laptops become more secure through tougher security standards and best practices, unprotected MFDs are a logical target for hackers and information thieves.

A carefully structured search of the Internet brings up enough “teaser” hits from hacker forums to suggest a growing interest in MFD weaknesses. One website describes how to use Google hacks – requests typed into the search engine that bring up cached information on networks – to discover and use login details for networked photocopiers in order to watch what is being copied.

“The threat landscape has evolved to include devices that when originally designed were never considered a security threat,” said Tom Moore, vice president of embedded sales, McAfee. “Now we are seeing the need for security on devices like MFDs to protect confidential and proprietary data which, if lost or stolen, could negatively impact a company and its employees.”

MFDs have evolved, adding more capabilities that bring significant benefits to the workplace and new security threats. Organizations need to be aware of those risks and take steps to secure MFDs so that the safety of the network and confidential data is not compromised.

Steps to Secure an MFD

To protect confidential information from security threats, it is a priority to apply security controls consistently across an organization when installing a multifunction device (MFD). When acquiring new equipment, select an MFD that is configurable and offers built-in security features. Ask vendors about security-related features and recommendations on installation and implementation. For existing equipment, contact the vendor about equipment upgrades that include security features.

Here are some tips for securing MFDs in your organization:

- Configure copiers, printers and other MFDs for improved security. Shut off any ports or features that you do not use.
- Place MFDs in secure areas if possible, and limit network access to systems administrators.
- Change the default administrator password, although it is recommended to use the same password for all MFDs for administrative efficiency. The copier dealer will need the password to perform maintenance — make sure that it is kept secure.
- Work with vendors to ensure devices meet industry security standards and certifications. Many vendors offer optional data security kits.
- Make sure IT staff and employees are aware of the organization’s data security policies and practices. Where possible, require that users enter a passcode or PIN to access spooled print or copy jobs.
- Perform firmware updates regularly.
- Consider requiring drive encryption. If possible, configure devices with hard disks to erase files after each print, scan, copy or fax job.
- Develop policies and procedures that address MFD disposal. Destroy or erase internal hard drives before decommissioning the device.

Making the Switch

Organizations need to prepare strategically for the transition to IPv6.

It's not exactly like the Mayan Apocalypse, or even Y2K. No tick of the clock is going to signal the end of the IPv4 Internet addressing system. But network administrators worldwide are facing the task of transitioning to IPv6, a project that requires careful planning to avoid business disruption.

The move to IPv6 is inevitable. IPv4's 32-bit addressing allows for about 4.3 billion unique IP addresses. That's simply not enough to accommodate all of the Internet-connected devices in use today. In fact, the pool of IPv4 addresses managed by the Internet Assigned Numbers Authority dried up in 2011, although a few regional Internet registries still have some IPv4 addresses available.

Using 128-bit addressing, IPv6 theoretically allows the creation of more than 340 trillion trillion trillion possible unique addresses. That's about a billion-trillion times larger than the total pool of IPv4 addresses, enough to give every human on the planet trillions of addresses of their own.

Although it has been available for a decade, IPv6 has been slow to catch on while IPv4 addresses were still available. Techniques such as network address translation (NAT), in which many of an organization's devices are hidden behind a single public IP address, have extended the life of IPv4. However, organizations need to make their networks compatible with the increasing number of IPv6 addresses. And if their websites and other web-based applications cannot be reached through IPv6, they are not accessible across the entire Internet.

Planning Ahead

The transition to IPv6 is not simply a matter of flipping a switch. IPv4 and IPv6 are different protocols and are not directly compatible, so programs and systems designed to one standard cannot communicate with those designed to the other. Techniques such as NAT further complicate the transition to the new protocol.

This doesn't necessarily signal the impending death of IPv4, however. Dual stack IPv4/IPv6 devices and software can help ease the transition by running both protocols simultaneously. Other strategies for making the transition include performing IPv6-to-IPv4 translation, tunneling, and using proxy servers to facilitate a migration to the new address space as software allows.

The latest versions of most enterprise-class network components and systems are already IPv6-capable. Still, most organizations have legacy equipment and applications that do not support IPv6 — a fact they must bear in mind as they plan future IT purchases. Experts also say firewall and security policies should be reviewed to determine how IPv6 will affect them, and in-house software should be upgraded to ensure compatibility. IPv6 should be tested in an internal lab to certify software, develop operational and support practices, and support transition planning.

Perhaps the biggest impediment to the IPv6 transition is the learning curve involved. Network engineers who are well versed in IPv4 shouldn't have much trouble learning IPv6. Nonetheless, IPv6 involves new concepts and functions in a very different way than its predecessor. Organizations should invest in training so that network administrators can become familiar with deploying and configuring the new protocol.

Great Potential

While network future-proofing and infrastructure management are the key reasons for transitioning to IPv6, businesses will be able to leverage the new protocol in a number of ways. At the most basic level, it supplies the additional IP addresses needed to accommodate the many smartphones and other Internet-connected devices flowing into the workplace.

There is also huge potential for new applications and devices that are IPv6-enabled. IPv6 will enable devices to multicast, which is the ability to send information and establish unique links to multiple devices without resending the same data to each device. That will make it easier to stream live video to multiple locations at once.

IPv6 also offers built-in security and enhanced support for streaming media and other Web 2.0 applications. In addition, the QoS features built directly into IPv6 can help improve the quality of encrypted Voice over IP calls.

The depletion of IPv4 address is not some impending doomsday. As IPv6 continues to gain momentum, however, organizations that fail to plan ahead risk finding themselves at a competitive disadvantage. Even if organizations don't have immediate plans to implement IPv6, preparing for the inevitable transition now as opposed to later will only decrease the burden on IT administrators.

IPv6 will open up a pool of Internet addresses that is virtually inexhaustible for the foreseeable future. Making the switch to this new protocol doesn't have to be daunting if a thoughtful approach is taken.

Unlike many other consulting firms, Verteks has developed unmatched expertise in several critical areas, which allows us to serve as a central source for a broad range of high-quality solutions to complex IT issues. Contact us today and let us show you how we can help you simplify your business with technology.

VERTEKS
VOICE & DATA
NETWORKS

1-877-VERTEKS 352-401-0909
www.verteks.com

ShoreTel®

ShoreTel Enterprise Contact Center is a powerful call center solution that puts business intelligence right where its needed. ShoreTel enables contact center functions and key business applications to be integrated onto a single, web-managed and highly available platform. Additionally, enhancements in ShoreTel Enterprise Contact Center 8 now make it easier to meet the needs of today's multi-device, multi-channel consumer by allowing agents to effectively handle emails, chats and calls, both inbound and outbound. Call Verteks to learn more how ShoreTel Enterprise Contact Center can help you improve your customers' experience.

VERTEKS
VOICE & DATA
NETWORKS

1-877-VERTEKS ■ 352-401-0909 ■ www.verteks.com

Copyright © 2013 ShoreTel. All rights reserved. SHR-13