

VERTEKS CONNECTION

MARCH/APRIL 2006



The Search Is Over

Furniture Country Galleries finds the right IT partner in Verteks Consulting.

What do you look for in an IT provider? Tina Gayler, Information Systems Manager for Furniture Country Galleries, expects her IT provider to be knowledgeable, experienced, responsive and thorough. After hassling with a number of less-than-qualified technicians, she found all of those qualities in Verteks Consulting.

"I called a guy I trusted and asked him to recommend a good technology provider. And he said, 'Call Verteks Consulting. They're wonderful,'" Gayler said. "So I called them, and I was happy with what they had to say. We decided to give them a try and



it's been a wonderful relationship ever since."

Talk Gets Cheaper

That was nearly five years ago. Since then, Gayler and the Verteks team have worked together on a num-

ber of projects that have brought cost savings, increased efficiency and reduced risk for Furniture Country Galleries. Chief among these projects was the implementation of a 3Com voice over IP (VoIP) system.

"As our company expanded we needed to look at new voice technology that could help us work a little smarter and save money in the process," Gayler said. "We talked to Verteks and determined that voice over IP was the best solution."

Because the VoIP system routes voice calls over Furniture Country Galleries' WAN, all of the company's locations operate with a single, unified

VERTEKS CONNECTION

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

continued on page 2

phone system. That saves long-distance charges between its stores in Ocala and Leesburg and warehouse in Wildwood.

“We communicate with each other a lot, so this system is saving us a substantial amount of money just on our internal calls,” Gayler said. “Plus, when our delivery department calls customers, the system routes those calls through the local store’s phone lines so it’s a local call.”

Many Benefits

The 3Com VoIP system provides other benefits as well. It enables Furniture Country Galleries’ staff to contact each other by dialing an extension versus a 10-digit phone number. It also provides each person with voice mail.

“We have a large sales staff, and taking messages for them was a huge headache,” Gayler said. “The voice over IP system enables us to set up voice mail even for people who don’t have a physical phone.”

The VoIP system is also easy to maintain. Gayler can handle many of the moves, adds and changes herself.

“The system we had previously was pretty antiquated and making modifications was difficult. I had to have somebody come in and help me,” Gayler said. “Now I can make changes myself — and if I have a question Verteks can usually talk me through it over the phone. It’s convenient and saves money because I don’t have to call somebody out every time I have a question or problem.”

Gayler says the VoIP implementation went smoothly, and that the system has worked well. She credits both 3Com’s technology and Verteks’ expertise with the success of the project.

“I did a lot of research going into this project and was concerned that there might be more issues than there turned out to be,” she said. “Verteks is very knowledgeable, very capable. Their technicians do a great job.”

Double Vision

The continued expansion of Furniture Country Galleries drove another IT project — the implementation of a redundant server and network-attached storage solution. The system is designed to help minimize downtime and improve data backup processes.

“We’ve been fortunate but downtime happens to everybody at some point. We wanted redundancy so that if we were down we could be back up in hours versus days,” Gayler said. “As a small business we have one primary server. If it goes down, we have three sites with more than 100 people who aren’t working. That’s a big concern.”

Verteks played a key role in helping Gayler design and

implement the redundant server solution.

“They did the legwork for me,” Gayler said. “They built a redundant server that had dual everything — from processors to hard drives to power supplies — to reduce the possibility of failure. They then built a secondary backup server so that if the primary server did fail we could restore a backup image and be back up and functioning within a matter of hours. They also designed a network attached storage solution so that I have a constant backup even if my tape backup fails.

“Verteks did another outstanding job implementing the new hardware and software. We were able to get everything done in the timeframe we had allotted.”

Look! No Wires!

Verteks has also helped Furniture Country Galleries take advantage of 3Com wireless network in its new warehouse facility.

“This solution enables our warehouse staff to use PDAs to access inventory information, do receiving and a whole host of things while they’re walking around the facility,” Gayler said. “The site plan Verteks developed was key. This is a large building — 60,000 square feet — and two-thirds of it is 40 feet tall. There is a lot of open space and also a lot of racks with product in them. We had some concerns about coverage, but Verteks came up with a great solution.”

The real magic with the 3Com wireless switching system is that it enables roaming. With other wireless systems, a user would have to manually reconnect to the network each time he moved to a different zone.

“With this system I have continuous network access no matter where I go,” Gayler said.

Proven Partner

Gayler says these projects exemplify the high quality work performed by Verteks’ technicians as well as the firm’s dedication to service. With about 50 end-users and a WAN to support, Gayler relies on Verteks for advice and support, as well as project-based work.

“I am the whole IT staff, and if I didn’t have Verteks I’d probably go crazy,” she said. “I can call them and if they can’t help me over the phone they are always willing and able to send somebody quickly — in some cases immediately. Every technician who comes out knows what he’s doing and sticks with the problem until he gets it resolved.

“I was very skeptical at first because I’d had bad experiences with technicians in the past. Verteks had to earn my trust but they’ve done a great job. I’m a big Verteks fan.”

Keyloggers on the Rise

In November, iDefense released data indicating that hackers were on pace to unleash a record-setting 6,191 keyloggers in 2005, a 65 percent increase from the 3,753 keyloggers released in 2004 and significantly more than the 300 in 2000.

Keyloggers, silently installed programs that record a victim's keystrokes and send them to hackers, put tens of millions of Internet users' finances, personal data and account information at risk. Largely distributed by organized cyber theft groups, they are typically packaged with phishing e-mails or spyware — malicious code that tracks victims' online activity — often eluding traditional security defenses such as anti-virus software and firewalls.

"Keylogging is a very effective

method for hackers," said Joe Payne, vice president, VeriSign iDefense Security Intelligence Services. "Fraudsters can launch hundreds of keylogging attacks around the world in seconds, gathering sensitive data to conduct large-scale monetary transfers for their illegal activities."

Once a keylogging program is activated, it provides hackers with personal data such as address, account numbers, mother's maiden name or passwords — any strings of text a person might enter online. Using this information to assume another's identity, hackers run up charges averaging \$3,968 per victim, according to a Nationwide Mutual Insurance Co. survey. Sixteen percent of victims were required to pay for at least some of this fraud, and spent an average of 81

hours to resolve their cases, reported the survey.

Hackers rely on a variety of techniques, including Internet Relay Chat and backdoor access to systems, to gather and filter logged keystrokes. Some groups create and sell keylogging programs to identity thieves, while others sell the stolen data. Still, others obtain the data and execute the fraudulent transactions.

"There are so many victims because so few know the risk or the early warning signs; you simply can't stop what you can't see," added Payne. "In addition to basic protections like up-to-date anti-virus programs and well-configured firewalls, the best defense for keylogging is to carefully track the organizations and hackers who promulgate these programs."

How Secure Is Your Business?



Detect vulnerabilities on your Internet-facing server and get a detailed security report on one publicly facing IP address with FreeScan, a free tool from Qualys and Verteks Consulting.

FreeScan allows you to quickly and accurately scan your server for thousands of vulnerabilities that could be exploited by an attacker. If vulnerabilities exist on the IP address provided, FreeScan will find them and provide detailed information on each risk — including its severity, associated threat, and potential impact. It even provides links to give you more information about the vulnerability and how to correct it.



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

Please visit <http://www.verteks.com/freescan> to request your free scan — there's absolutely no risk and no obligation.



Copyright © 2006 Qualys, Inc. All rights reserved. QLY01

Intruder Alert

Intrusion prevention systems help thwart network attacks.

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 network firewalls have supplanted the castle wall and moat, and do a pretty good job of keeping out most of the traffic that may pose a threat to the organization. However, most firewall policies specifically allow any network traffic — SMTP, HTTP, FTP, etc. —the organization needs to do business.

Some organizations do post a sentry, known as an intrusion detection system (IDS). However, this sentry isn't able to operate the drawbridge. An IDS is a passive system that sits outside the data path looking for possible attacks within the traffic allowed through the firewall.

Intrusion prevention systems (IPSs), in contrast, sit inline to effectively monitor and block malicious traffic. While IDSs spot incoming attacks and notify administrators, IPSs go a step further by stopping attacks before they make their way into the network. Because IPSs operate within the data path, they can actively drop packets when malicious activity is identified.

Know Thy Enemy

Such activity remains top of mind among organizations of all sizes. In a recent survey conducted for Nortel by Mindwave Research, 43 percent of respondents fear hacking the most, followed by viruses, worms and Trojan horses. Over the past year, 57 percent had actually experienced a virus attack.



In another recent national security survey conducted by Top Layer Networks, 54 percent of respondents said they had experienced a cyber attack, with 21 percent projecting damages caused by these attacks exceeded \$100,000. Forty percent of respondents identified spyware as the most significant upcoming, 29 percent said worm infections and 24 percent named Distributed Denial of Service (DDoS) attacks.

Although 25 percent of respondents spend more than \$100,000 annually to secure their IT infrastructure, 35 percent feel that their existing security infrastructure does not adequately protect their servers, and 38 percent feel that it doesn't adequately protect their desktops. When evaluating network security products,

respondents identified the top three purchasing factors as protection (66 percent), reliability (63 percent) and performance (40 percent). IPSs (38 percent) outperformed IDSs (36 percent), as more respondents have come to realize that blocking attacks is preferable to just detecting them.

Ongoing problems with viruses, worms and hacker attacks point to the limited value of IDSs. While it is important to know when an attack is in progress, such notification is not sufficient protection against rapidly spreading attacks. Organizations need inline IPS technology that can both notify of attacks and thwart a potential security breach before it can adversely impact a business.

Halt! Who Goes There?

When one thinks of an intrusion, one generally thinks of unauthorized network or application access with the intent to steal or destroy valuable information. However, unauthorized access isn't the only intrusion blocked by an IPS.

IPSs use a wide range of techniques — including signature matching and protocol and traffic anomaly detection —

to protect against malicious content such as viruses and spyware. IPSs provide real-time protection against malicious content attempting to enter the network data stream.

IPSs also protect against rate-based attacks such as DDoS attacks. Such attacks, which attempt to flood a network with seemingly legitimate traffic in order to overwhelm it, are often perpetrated for financial gain — hackers will threaten an organization with a DDoS attack unless a ransom is paid. IPSs block rate-based attacks through advanced techniques that distinguish legitimate from seemingly legitimate traffic.

“Securing critical IT infrastructure by not only preventing undesired access and protecting against malicious content that exposes private data, but also stopping rate-based attacks that can be employed for extortion purposes are all key considerations in working toward fulfilling compliance and client expectations,” said Peter Rendall, CEO and

President of Top Layer Networks.

Legal Mandate

Protection against DDoS attacks in particular is vital given today’s regulatory climate. Nearly two-thirds of organizations polled by Top Layer Networks cited that they must comply with at least one government regulation such as HIPAA, Gramm Leach Bliley or Sarbanes Oxley, and compliance was a key driver in security purchases.

The Gramm-Leach-Bliley Act (GLBA), for example, requires U.S. financial institutions to ensure the security and confidentiality of customer records and related information. As part of this act, the five federal banking agencies and the Federal Trade Commission have provided guidelines for developing and implementing safeguards to protect the confidentiality, integrity, security and availability of customer information. Financial industry experts from the ReymannGroup have stated unequivocally that banks

should have an ability to protect against DDoS attacks to comply with GLBA.

“A proactive DDoS risk mitigation strategy is not just best practice — it’s mandated.... Clearly the intent of existing laws and rules such as Sarbanes-Oxley and GLBA is to insure against known external threats to an organization’s network. DDoS attacks are a real threat to the integrity and secure availability of confidential client data and financial institutions must have prevention plans in place,” said Paul Reymann, CEO of ReymannGroup and the co-author of the GLBA data protection regulation.

IDSs are effective at preventing these kinds of attacks but they’re not a panacea. Experts recommend a layered defense that includes perimeter firewalls, e-mail gateway scanning, desktop anti-virus protection and other security components. However, Like a sentry posted at the castle gate, IPSs can not only detect attacks but prevent intruders from gaining access to the network.



A complete, affordable network solution for small businesses

As a small business, you have limited time and resources to get the job done and keep your business running. Technology can simplify your daily activities while saving you time and money.


VERTEKS
VOICE & DATA
NETWORKS

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

Designed with your company needs in mind, Windows Small Business Server 2003 is a complete and affordable network solution. With Windows Small Business Server 2003, you can have confidence that your data is secure, untap new productivity from your desktops, empower your employees to do more, and connect to your customers like never before. Call Verteks today to learn more.


Microsoft
GOLD CERTIFIED
Partner

Copyright © 2006 Microsoft Corporation. All rights reserved. Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States and/or other countries. MS-65

Accelerating WLANs



New proposal to improve speed, coverage of wireless networks.

The recent approval of a new high-speed wireless networking proposal opens the door for bandwidth-intensive services such as Voice over IP (VoIP) and streaming video to run over WLANs, industry experts say. Although ratification of a final standard likely won't occur for another year, one analyst firm predicts that sales of equipment based on the standard will exceed \$1 billion by 2007.

After months of wrangling between rival industry factions, the Institute of Electrical and Electronics Engineers (IEEE) — the standards body for the electronics industry — voted in January to accept a working draft specification for the emerging 802.11n standard for wireless networking. With actual throughput speeds of 100Mbps, the proposed 802.11n wireless standard will be up to 40 times as fast as some current wireless networks based upon the commonly used 802.11a/b/g standards.

The Dell'Oro Group, which is forecasting a rapid upswing in 802.11n sales, said it expects the new standard will comprise 90 percent of consumer WLAN shipments by 2009. The analyst firm expects enterprises to begin widely adopting 802.11n once this new technology has become established in notebook computers.

“The IEEE's recent approval of a draft 802.11n standard was sorely needed,” said Greg Collins, senior director of WLAN research at Dell'Oro Group. “In recent quarters the consumer market for WLAN equipment has stagnated,

especially from a revenue perspective, because 802.11g-based products have been in the market for three years, and consumers have not seen a cost-benefit to upgrading to 802.11a. Due to its better coverage and higher data rates, 802.11n will likely become a key enabling technology for distributing video to multiple devices in the home.”

Finding MIMO

In theory, 802.11n will be up to 40 times faster than 802.11b, and almost 10 times faster than 802.11a or 802.11g. That substantial boost in speed comes thanks to a technology called MIMO — short for multiple input, multiple output. MIMO uses multiple antennas to transmit and receive data in the unlicensed 20MHz to 40MHz frequencies. By using four transmit and four receive antennas, for example, MIMO can quadruple the raw data speeds.

In addition to transmitting data much faster than existing WLAN technologies, 802.11n promises to deliver eight times the coverage, enabling very high-speed connections over distances of 300 feet or more. That is essential to providing the bandwidth and quality of service needed to run advanced applications, such as streaming video and VoIP.

The addition of an 802.11n device can improve the performance of existing 802.11a/b/g networks because it does not drop to the lowest common networking speed in mixed-mode environments. It also resists interference from neighboring Wi-Fi systems and 2.4GHz devices.

"Now that we have the technical foundation for the 802.11n standard, the Wi-Fi market will begin to experience renewed growth as vendors deliver next-generation wireless devices," said Philip Solis, senior analyst at ABI Research. "We expect suppliers ... to capitalize on this opportunity by introducing advanced solutions that promise interoperability and upgradability when the standard is completed, just as it did with its draft 802.11g solutions."

Caution Urged

Since final ratification is not due until late 2006, some analysts say organizations must use caution in evaluating any products claiming to be "802.11n compatible." Several vendors have already announced that they will start producing "draft-compliant" chipsets, but analysts at Gartner have labeled these claims as "misleading" and "premature." Gartner noted that the technology is likely to be changed before a final standard is approved, and that additional testing will be required to ensure compatibility with

existing Wi-Fi standards.

ABI Research's advice to vendors and customers is to expect draft-compliant equipment as early as the first quarter of 2006, but more likely in the second quarter.

"Silicon vendors claim that their draft-compliant chips will be

firmware-upgradeable to the eventual ratified standard," said Sam Lucero, ABI Research senior analyst of wireless connectivity research. "Initially this will mostly be consumer-oriented equipment; we believe that enterprise IT managers will not purchase equipment until the standard is actually ratified."



3Com® Wireless: Meeting the needs of your mobile workforce

To meet the needs of an increasingly mobile workforce, businesses today require a wireless solution that also combines security and reliability in one complete package.

With the strongest encryption available, no dropped connections and QoS for data, voice and video applications, 3Com enterprise class solutions provide businesses with any size network, Internet access without the wires and without the worry.

And, as your 3Com authorized reseller, you'll be backed by first-class service and support, to ensure your wireless solution meets your needs today and into the future.

Verteks Connection

Copyright © 2006 CMS Special Interest Publications. All rights reserved.

Editorial Correspondence:
4941 S. 78th E. Ave., 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.


VERTEKS
VOICE & DATA
NETWORKS
1-877-VERTEKS
352-401-0909
www.verteks.com


security
VoIP
wireless
switching
routing
services

Copyright © 2005 3Com Corporation. All rights reserved. 3Com and the 3Com logo are registered trademarks of 3Com

COM-18

Do the math...

1 wire for all your voice and data needs
1 system ties together all of your locations
1 wise investment that increases employee productivity

1 + 1 + 1 = The 3Com family
of IP Telephony Solutions



The 3Com NBX V3000 platform provides the benefits of convergence applications to enterprises with from 2 to 200 users and up to 1,500 devices. It eliminates the cost and administrative overhead required for separate voice and data networks and affordably improves communications with powerful built-in call-processing, messaging and reporting features. Call today to learn how you can trade-in your old voice system and take advantage of these powerful capabilities.



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