VERTEKS
CONNECTION

AUGUST/SEPTEMBER 2007

VERTEKS
VOICE & DATA
NETWORKS

One Call Does It All

Verteks serves as a one-stop IT resource for Highland Tractor.

Information technology is undeniably complex, but that doesn't mean vendor relationships have to be. For Highland Tractor, Verteks Consulting serves as a one-stop resource for its technology needs.

Although Highland Tractor has a skilled network engineer on staff, Verteks plays a key role in the firm's IT strategy. The Ocala, Fla.-based purveyor of construction, forestry and turf equipment looks to Verteks for sound advice, technical expertise and help with complex projects.

"Like any business in this day and age, we rely on computers for every aspect of our operations. And our IT needs continue to expand as our business grows," said Randy Fitts, General Manager, Highland Tractor. "Verteks knows the best solutions available and, more importantly, how to put them to work for our organization. They're a great resource for us."

Solid Foundation

Highland Tractor has turned to Verteks for a wide range of projects, including the implementation of a 3Com NBX IP phone system. The 3Com solution replaced an antiquated four-line phone system that lacked the functionality Highland Tractor needed to support its business growth.

continued on page 2

VERTEKS CONNECTION

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

"The 3Com phone system has given us a stable voice communications platform that interfaces with the computer network," said Pete Kamay, IT Director for Highland Tractor. "It's very user friendly and provides us with voice mail, call monitoring, call reporting and other features we need."

Verteks deployed the 3Com system at three of Highland Tractor's eight locations. The system has been so successful that a company-wide roll-out is in the works.

Kamay says the system will ultimately reduce long-distance costs by tying all of the locations together. Simplified administration is another key selling point.

"Sitting right here in Ocala I can take care of any phone needs at our remote branches. Moves, adds and changes are so easy," Kamay said. "Just this morning, our general manager asked if he could check his messages from other extensions and have calls go to his cell phone while his office is being renovated. I was able to take care of that for him in a couple of minutes."

A Helping Hand

The 3Com system is scalable and easy to upgrade — a real boon to an organization that continues to expand. In 2006, Highland Tractor added a new wing to its corporate office and needed 30 new phones as well as conferencing capabilities. All Kamay had to do was enter the new license codes, and the phones were operational.

That's not to say that Verteks wasn't involved in the expansion. Highland Tractor called on Verteks to install all of the network cabling in the new facility, and to install a fiber-optic link to their existing building.

"Cabling can be very challenging, but Verteks is so fast and efficient — it only took them a couple of days to run about 120 network drops in the new wing. They have it down to a science," Kamay said.

"Anything that's impractical for us to do internally — because we lack either the skills or the time — we turn over to Verteks. They have a wide range of capabilities, a highly trained team and competitive rates. Verteks is the only place we have to call."

The Right Stuff

Training and certifications are important, of course, but the practical knowledge that comes from helping solve real business problems sets Verteks apart.

When Highland Tractor needed a better way to connect its branch locations to the central office, Verteks recommended using a WatchGuard firewall with virtual private network (VPN) capabilities to create secure "tunnels" via the Internet. Because Verteks had successfully deployed the WatchGuard system in similar situations, Highland Tractor was confident it was the right solution.

"We were using older technology to connect three stores but as we started adding more locations it just couldn't keep up," Kamay said. "I called Verteks, confident that they would know what we needed. I didn't have to do any research — I just told them the situation and they recommended WatchGuard. They said, 'We've installed this before and we know it works.' And it does. The system has been rock solid, and it's easy for users at the remote locations or even at home to log into our system."

Technology can be complex, but Verteks has the knowledge and experience to make it work seamlessly. And, best of all, area businesses have just one number to call for the IT help they need.

"I know this network better than anyone and I know what our business needs are. But there are also times when I need outside assistance," Kamay said. "Verteks has already done the research, and has already implemented these technologies in other facilities. They know the potential pitfalls and workarounds for any snags that might come up. They're very efficient and easy to work with, and they get the job done."

"Anything that's impractical for us to do internally — because we lack either the skills or the time — we turn over to Verteks. They have a wide range of capabilities, a highly trained team and competitive rates. Verteks is the only place we have to call."

— Pete Kamay, IT Director, Highland Tractor

Business Wireless Investments Set to Skyrocket, Analysts Say

Enterprises are poised to expand their wireless investments considerably over the next 12 to 18 months, according to a recent benchmark report from Nemertes Research. The firm predicts that organizations will increase the number of mobile devices they use by an average of 421 percent over that time frame.

Companies are investing top dollar to enable employee mobility: Organizations with revenues of more than $1 billion report spending a median of $5,000 per year per mobile-enabled user. For PDA users, the median spend is $5,357; and for wireless laptop users, the median spend is $4,611.

"Crafting a mobility strategy is a key priority of benchmark participants, with 60 percent of enterprises indicating they currently have or are planning adoption of a mobility strategy," said Johna Till Johnson, Nemertes president.

Multi-mode and multi-function devices are another key for IT executives: 75 percent of benchmark participants say they're interested, or somewhat interested, in multimode products — devices that handle both WiFi and various flavors of wireless-WAN services.

New broadband wireless technologies including WiMax will keep spending on enterprise wireless LAN equipment in double digits over the next five years, according to a recent study by Gartner. The firm predicts the market will grow at a compound rate of 17. 3 per cent worldwide and hit US$3.1 billion in 2011

Verteks Connection

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.

Wireless and Secure

Effective WLAN security requires a layered approach.

There's no question that wireless LANs (WLANs) offer compelling benefits in terms of mobility and productivity. In a recent Web poll conducted by the Computing Technology Industry Association (CompTIA), 13.1 percent of technology professionals surveyed said that wireless data applications would have the greatest impact on their organizations this year — the second most popular choice.

Security solutions ranked No. 1 in the survey, chosen by 24.3 percent of IT professionals. WLAN security is particularly problematic, creating a major stumbling block that prevents organizations from fully reaping the rewards of wireless.

However, it is possible to balance mobility with robust infrastructure security. While some organizations have chosen to focus on the risks associated with WLANs — to the point of banning the technology — many others have successfully deployed wireless networks that are as secure as the wired infrastructure.

The Layered Approach

The key, according to experts, is to take a layered approach to WLAN security by identifying and protecting against wireless-specific vulnerabilities. All too often, organizations focus on one area of WLAN weakness — such as inadequate encryption — while failing to see the big picture.

Effective WLAN security depends upon a comprehensive framework covering all aspects of the wireless infrastructure, from the radio frequency (RF) layer all the way to the application layer. Organizations must put tools in place that check for rogue devices entering the airspace, attacks on wireless links, and unauthorized users attempting to access the network.

This requires a mix of security solutions based upon industry standards along with continuous real-time monitoring and policy enforcement. Network administrator must learn what to look for and effective ways of addressing WLAN vulnerabilities.

The lure of wireless combined with the ease with which it can be deployed represents one of the biggest threats to WLAN security. For a small investment, an end-user can introduce a consumer-grade wireless access point into the network, exposing the entire infrastructure to easy attack. Wireless-equipped laptops can pose an even greater threat is not properly secured.

Know Your WLAN

The first step in securing the WLAN is to find rogue access points and either eliminate them or ensure that they meet security standards. Many network administrators will use a handheld "sniffer" and walk through the WLAN coverage area looking for wireless data transmissions. However, experts say this is one of the least effective ways of eliminating rogue equipment — new rogue access points can be added after the scan.

A better solution is 24x7 monitoring of the WLAN for security risks. This enables the network administrator to know immediately when and where a rogue access point is deployed, and also identify new vulnerabilities.

Strong authentication and encryption are needed when user credentials and data are being broadcast through the airwaves. The Wi-Fi Protected Access 2 (WPA2) encryption standard offers substantially greater protection than the notoriously vulnerable Wired Equivalent Privacy (WEP) standard.

Intruder Alert!

The next step is to ensure that the WLAN is protected against attack. Experts recommend that organizations install WLAN-specific intrusion detection systems (IDSs) to keep hackers from accessing the wired network via the WLAN.

WLAN IDSs continuously monitor 802.11 protocols for security policy violations, known attack signatures and statistical anomalies. They are able to detect and thwart man-in-the-middle attacks, MAC spoofing and unusual activity.

Security software should be installed on all wireless-equipped devices to alert the network administrator of any vulnerabilities. Only enterprise-class access points with robust security should be used, and they should be configured to limit which stations can connect to them.

The Service Set Identifier (SSID) — the name of the access point — should be changed from well-known factory presets. In addition, the default SSID broadcast mode should be turned off so that only user stations that know the SSID can connect to the access point.

What's Your Policy?

It's critical that organizations develop — and enforce — a WLAN security policy. Robust WLAN security depends upon the installation and use of security software on individual clients, and the proper configuration of access points and stations. A WLAN security policy should establish these requirements and prohibit users from circumventing these measures.

A WLAN security policy must be flexible in terms of the technologies it can support. WLANs enable access by laptops, PDAs, smart phones and more, each with different features, capabilities and security requirements. This diverse set of clients cannot be secured with a "one size fits all" policy.

In addition, most WLANs are designed with end-user mobility and productivity in mind. The challenge for IT staff is to develop security options that support end-user requirements.

Finally, WLAN security policies must integrate with the organization's wired network security scheme to ensure seamless protection across the organization. While WLANs present unique security challenges, it still boils down to controlling who has access to specific information. Understanding WLAN-specific vulnerabilities and deploying a suite of tools to minimize them enables organizations to enjoy the mobility and productivity benefits of WLANs without putting business-critical applications at risk.

A Unifying Force

Unified communications combines voice, video and data to improve collaboration and productivity.

In the beginning there was an inbox, and it was good. Soon, there were multiple e-mail inboxes, multiple voice mail inboxes, cellular phone inboxes, pagers, PDAs with both e-mail and voice mail — not to mention the old-fashioned, cubby-hole-style inboxes next to fax machines. Not so good.

Today, however, the concept of voice, video and data as distinct elements of business communications is rapidly fading. The emerging trend toward unified communications is fundamentally changing workplace interactions by seamlessly blending a host of formerly independent communication applications.

"The rising popularity of collaborative social networking sites such as MySpace, video content sites including YouTube, and IM and VoIP clients from Microsoft, Yahoo!, Google and Skype, shows that the way people interact with one another in their personal lives is changing," said Matthew Ball, an analyst with Canalys, a technology convergence consulting firm. "And we will see more and more employees having expectations of similar rich-media collaborative applications, offered by unified communications solutions, for day-to-day working."

Beyond Messaging

The idea of unified communications is not all that new — for years, major technology and telecom companies have been eyeing ways to integrate faxes, e-mails and voice mails into a single inbox. But with the growing popularity of converged voice and data networks, unified communications is emerging as a key application for taking advantage of convergence.

Beyond merely integrating messaging applications, unified communications adds features such as real-time call control, collaboration, media handling and further integration of voice and data applications. The newest unified communications systems provide opportunities to integrate instant messaging (IM), presence awareness, features such as click-to-call, click-to-conference, Web and voice conferencing, Web or multimedia chat, and document collaboration. By integrating these various technologies, unified communications systems can do more intelligent routing based on what's on the user's calendar, their presence status, and personal rules.

"Over the last five years, we have seen the rate of converged voice and data network deployment increase significantly, especially in medium-sized and large businesses. These businesses want to build on their investments and start looking at the way employees communicate within teams, and with customers and suppliers, to make them more efficient and productive," said Ball. "Telephony will be increasingly integrated with user presence and identification, as well as other modes of communication, including e-mail, instant messaging, video and Web conferencing — all of which are accessible through a multitude of software clients, business applications and end-user devices."

'Voice over Everything'

One feature of unified communications is the ability to embed voice capabilities in all sorts of applications — a concept often referred to as "Voice over Everything." The idea is to incorporate everything from voice-activated documents to voice mails in e-mail inboxes. At the click of a button, users will be able to speak to people who are working on a jointly written document to make amendments, reply verbally to e-mails, or check a person's availability. VoE will increase productivity by reducing the length of time it currently takes to make phone calls. Users will simply click on links within IT applications without dialing, looking up numbers in a directory or having to organize conference calls. Analysts say VoE will also save businesses anywhere from 15 percent to 30 percent on telephone costs.

"Today we dial; tomorrow we click," said Geoff John-

son, research vice president at Gartner. "Voice will be embedded in everything and mobility will be crucial. Calls will be made by clicking through a document or an e-mail rather than dialing a number."

The Session Initiation Protocol (SIP) has been the key to rapid rise of unified communications applications. SIP is a signaling-type protocol that enables different types of devices such as computers, handheld gadgets and telephones to "talk" with each other seamlessly in an IP network. Because SIP is an Internet Engineering Task Force (IETF) protocol, it is inherently an open architecture, which is a big reason most major communications equipment manufacturers and software companies are embracing it.

Although SIP is used to enable IP telephony, it is not merely a software-based telephony switch — it is capable of much more than that. SIP treats voice as just another medium, albeit a very important one. It can also be used to send files such as video images between two points, opening the door for a variety of multimedia applications. It is quickly becoming the backbone protocol for numerous personal and enterprise communications such as rich-media conferencing, push-to-talk and location-based services.

Present and Accounted For

Presence technology is another key element of unified communications platforms. Voice-embedded applications leverage presence just as IM uses the technology to allow users to see whether someone is available, busy, away from their computer or offline. Because presence-based applications leverage real-time information about user, system or device availability, they can determine an intended recipient's location and route information to the appropriate computer or device, guaranteeing that the user receives critical information in a timely manner.

Presence technology not only supports communication between users, but application-to-application integration in which the presence infrastructure announces which applications are up, what their functions are and what types of protocols they accept.

"Our vision for unified communications breaks down today's silos of communication and brings them together into an intuitive experience that puts people at the center," said Zig Serafin, general manager of Microsoft's Unified Communications Group. "By ensuring interoperability with business-grade communications capabilities from leading providers, we can extend the power and flexibility of software to improve phone-based communications."

PHONE SYSTEM GOT YOU DOWN?

SHORETEL WILL MAKE YOU JUMP FOR JOY

Step up to ShoreTel. Finally, there's an intelligent IP phone system out there that offers you a choice and flexibility, translating into unprecedented freedom and improved productivity for everyone—end users, IT staff, and managers.

"ShoreTel was so easy it made us wonder what the telco experts were feeding us all those years. You install it and it works."
Derrick Crandell, Director of IT
BKF Engineers

Contact Verteks today for more information about ShoreTel's IP Telephony Solutions.

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

ShoreTel
www.shoretel.com

VERTEKS
VOICE & DATA NETWORKS

SHR-05