

VERTEKS CONNECTION



volume 12 number 1

Smart Strategy

As its technology needs grow, Meadowbrook Academy relies upon the experts at Verteks for IT services and support.

Technology is playing an ever-larger role in K-12 education as schools seek to engage today's tech-savvy students. Meadowbrook Academy recognized this trend several years ago, and began developing the IT infrastructure needed to support and enhance its academic programs. Today, the Ocala, Fla., school uses technology extensively in its classrooms, and relies upon Verteks Consulting to keep its IT environment up to date and running smoothly.



Meadowbrook Academy was founded in 1996 as a ministry of Meadowbrook Church, and both organizations relied upon a shared in-house IT team. Over time, that team grew to include multiple help desk technicians, system administrators and managers.

Verteks was called in to assist with large projects and complex issues.

The academy began to grow and dramatically increase its use of technology. At the same time, several members of its IT team moved on to other opportunities. The remaining IT staff struggled to keep up with the volume of support requests.

“The academy went from a very small computer lab to a hyper-acceleration of technology initiatives,” said Steve Maze, IT Director, Meadowbrook Church and Academy. “It didn’t take long before we were buried. At one point we had more than 250 open tickets, some of which were very old. We were not keeping ahead of demand for new computer systems, existing

continued on page 2

VERTEKS CONNECTION

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

continued from page 1

computer support and all the things the organization needed.”

Verteks proposed a co-managed IT program in which Verteks would provide remote monitoring and management and help desk support, along with sound advice and guidance. Verteks would serve as an extension of Meadowbrook’s IT team, enabling in-house staff to focus on strategic initiatives.

“It just made good sense,” Maze said. “The academy’s IT needs had outgrown our capabilities by a good measure. It put us in a place where we needed somebody better qualified to come in and help us. Verteks has a strong bench of people who have expertise in every aspect of the IT infrastructure — a sort of ‘brain trust.’ Instead of trying to keep a deep bench on staff, we knew this was the avenue to take.”

On the Front Lines

Verteks set up an end-to-end program that would keep Meadowbrook’s systems running smoothly. Meadowbrook even eliminated its in-house help desk ticketing system, instead relying upon Verteks to track and manage support requests.

“Verteks became the front line,” said Maze. “We presented to our staff that support is going to come from Verteks, not our in-house staff. We explained that there are several different avenues for requesting support — you can call the Verteks help desk or send an email — but you need to follow that process, even if it’s an emergency. It took a while for people to get used to it but it has worked out very well.”

Principal Tina Stelogeannis says that Verteks’ support enables teachers to focus on their students rather than troubleshooting technical problems.

“If our teachers have any IT issues they can contact Verteks and get a response immediately,” she said. “The technicians will even work around class

schedules because they know the teachers are instructing. Sometimes they can remote in and troubleshoot issues, which saves us a lot of time.”

Verteks’ support has become increasingly valuable as the school’s technology initiatives have continued to expand. Two years ago, the school began using tablets in its high school classes — first in the 11th and 12th grades, then the following year in the 9th and 10th grades.

“That was a big undertaking and Verteks really helped us out,” said Stelogeannis. “Knowing that we had experts available took the pressure off me administratively because that’s not my area of focus. The folks at Verteks are easy to talk to and always keep me up-to-date. They put every foot forward and burned the midnight oil to help us get it done.

“This year, we’re going to all-digital curriculum for the high school, and their guys have worked hard to get all of it uploaded. They went directly to our publishers to get the information they needed so I could focus on the new school year without worrying about technology questions. That’s one of the special things I really appreciate about them.”

Making Progress

The Verteks team also recommends new technologies that can save money, reduce risk and enhance Meadowbrook’s IT infrastructure. Maze points to data backup and security as two key areas where Verteks’ insight has proven invaluable.

“One of the holes in our infrastructure was a meaningful backup system. In fact, when the Verteks team performed the initial assessment before launching the managed services program, they pointed out that our backups were painfully lacking,” he said. “We had limited our backups to our

most important servers but even then we weren’t backing up every server due to the nature of the backup software we were using. Plus, our teachers had all kind of work product stored on their local machines. A hard drive failure would have been a nightmare.

“Verteks helped us develop a strategy for backing up all the teachers’ data onto a server, and then implementing new hardware and software for backing up everything in the data center. We have snapshots going back several months — I was able to restore some critical data for our vice principal because of that.”

When the school’s firewall license came up for renewal, Verteks recommended WatchGuard because it provides more comprehensive security. The WatchGuard solution could be tailored to the school’s needs, such as protecting the tablets and ensuring that students cannot access inappropriate content. Verteks also helped ensure that Meadowbrook was taking appropriate steps to protect credit card data.

Verteks has completed many other projects for Meadowbrook Academy, including implementing a new phone system and consolidating several physical servers onto virtual machines. Through Verteks’ expertise, insight and commitment, the school has developed a robust IT infrastructure capable of supporting its 21st-century education initiatives.

“As more and more of what we do becomes electronic, we have to have ongoing help,” said Stelogeannis. “We could not go where we’re headed with technology without Verteks.”

“So many of the things Verteks does ... you can’t really put a number on,” Maze said. “I appreciate the value of what Verteks has brought because we’ve grown tremendously and we’re not slowing down.”

News Briefs

5GHz to Fuel Wi-Fi Chipset Demands

More than 20 billion Wi-Fi chipsets will be shipped during the next five years as Wi-Fi solutions branch out into new usage scenarios, frequency bands, device types and performance requirements, according to a new report from ABI Research.

The firm says the migration to the 5GHz band will drive much of this activity, with more than 95 percent of devices shipped in 2021 to support 5GHz.

ABI says the new 802.11ax standard under development will account for 57 percent of Wi-Fi chipsets by 2021. However, with 802.11ac, 802.11ax and new LTE-U devices all tapping into the 5GHz spectrum, the firm says there are concerns over coexistence among the technologies going forward.

Wi-Gig, which offers high download rates and support for beamforming, will remain a premium standard for the foreseeable future, ABI says. The firm says HaLow, which aims to use Wi-Fi to connect Internet of Things networks, will be a longer-term bet because of competition from low-power wireless technologies such as LPWAN.

Survey: Intellectual Property at Risk

A majority of companies have no idea where mission-critical information is located on the corporate network, who has access or what is being done with that information, according to a new study. Additionally, few organizations have technology in place to keep employees from sharing confidential documents.

The sobering look at how companies protect intellectual property is described in a Ponemon Institute survey titled, "Risky Business: How Company Insiders Put High Value Information at Risk." The study was sponsored by IT security firm Fasoo.

The study finds that 72 percent of the 637 U.S. IT security practitioners surveyed are not confident in their ability to manage and control employee access to confidential documents and files. Almost 70 percent of respondents do not know where confidential information is located and more than 60 percent don't have visibility into what confidential documents and files employees are sharing.

Verteks Connection

Copyright © 2016 CMS Special Interest Publications. All rights reserved.

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.

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.

Your Behind-the-Scenes IT Team



Managed IT services from Verteks provide you with more reliable performance and more predictable expenses. That means you get more value from the technology you've already invested in, while actually reducing the total costs of IT problems and the resulting downtime. With managed services from Verteks, you can expect:

- **Reliability** – 19 years in business in Central Florida
- **Peace of mind** – your systems are monitored 24/7
- **Less downtime** – we identify and fix issues before they cause problems
- **Fewer disruptions** – we provide most services remotely or overnight
- **Predictable budgeting** – all-inclusive, all-you-can-use, flat-rate IT services that include hardware and software.

Contact us today to learn more.



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

day” 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, validation 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.

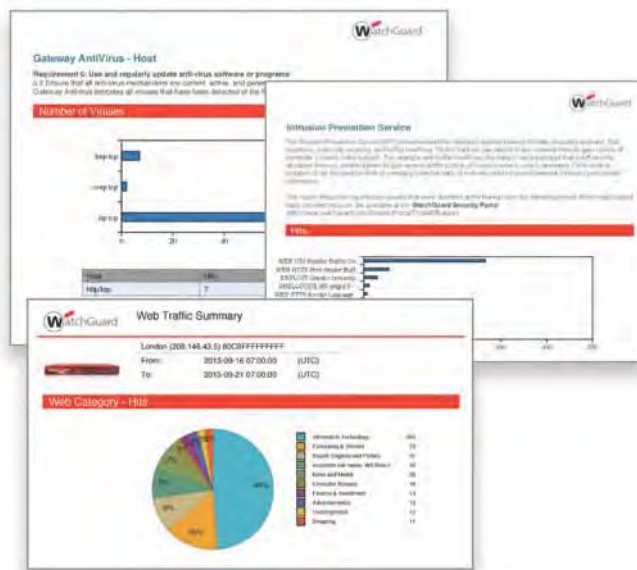
Standardize systems as much as possible. Most companies have more than one operating system to manage, increasing the number of patches to be applied. Reducing the number of platforms eases the patch management burden and helps reduce the possibility that applied patches will adversely affect other systems.

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.



Are you seeing the Big Picture?



WatchGuard Dimension™ is a cloud-ready network security visibility solution that comes standard with WatchGuard's flagship Unified Threat Management and Next Generation Firewall platform. It provides a suite of big data visibility and reporting tools that instantly identify and distill key network security threats, issues and trends, accelerating the ability to set meaningful security policies across the network.

WatchGuard Dimension helps you spot patterns and make better decisions with network activity presented visually, in real-time, in intuitive and interactive dashboards and reports. The elegant visualizations make it easy to identify potential threats, monitor Internet usage and to gain critical insights about related traffic trends.

Contact Verteks to learn more.



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

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 fre-



quently 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 overwhelmingly 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 overwhelmingly 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.



Business VoIP with the industry's highest customer satisfaction & lowest TCO

You owe it to your company to check out ShoreTel.

Streamlining the work of IT staff and users alike, ShoreTel's unified communications phone system provides:

- **MANAGEMENT EASE** – It's plug-and-play, maintainable from anywhere on the network
- **UNPARALLELED USER EXPERIENCE** – call control like never before with full feature access, including IM, mobility, video, and collaboration tools
- **ABSOLUTE RELIABILITY** – 99.999% availability for 100% peace of mind with the best customizable business continuity strategy in the business
- **ROI** – Many customers say their ShoreTel system pays for itself within a year
- **THE SUPPORT YOU NEED** – Independent surveys, industry awards and carefully monitored feedback from customers confirm it

Contact Verteks to see how ShoreTel's unified communications system will change how you view your business phone system.

