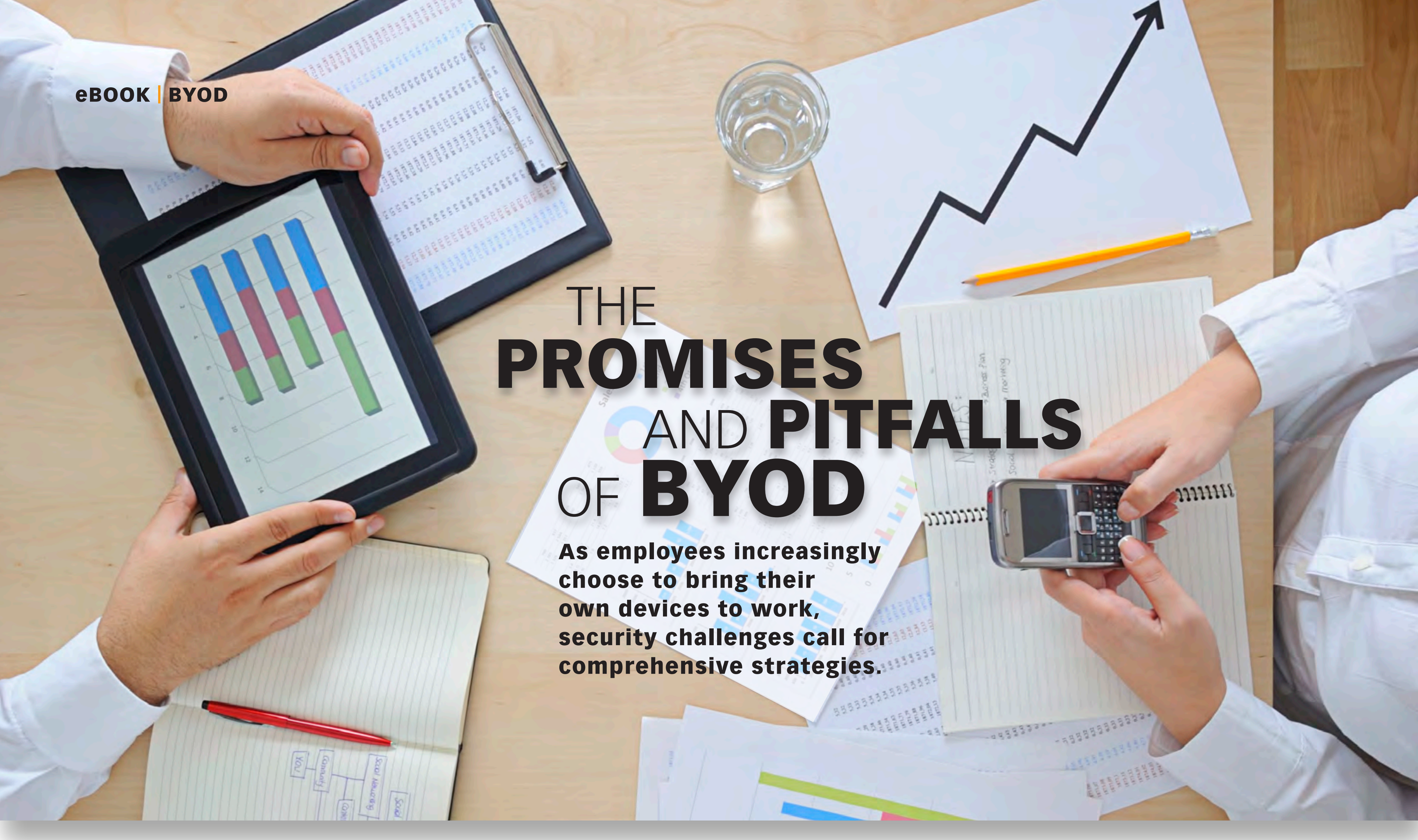

eBOOK | BYOD

THE PROMISES AND PITFALLS OF BYOD

As employees increasingly choose to bring their own devices to work, security challenges call for comprehensive strategies.

SONICWALL®

InfoWorld Custom Solutions Group

COMPUTERWORLD Custom Solutions Group

NETWORKWORLD Custom Solutions Group

INSIDE

The Bring Your Own Device (BYOD) trend is in full swing, as enterprises are beginning to realize a number of benefits from letting employees choose the device they use to get their jobs done. According to the *Computerworld* "Consumerization of IT" study published in October 2011, about half of the 604 respondents said their organizations allow employees to do work using their own devices either away from the office or at work. These companies know that by allowing employees to use personal devices they are improving productivity and job satisfaction. What's more, enterprises can significantly reduce costs as well as embrace the concept of virtual teams by leveraging geographically dispersed talent. Businesses can also allow for flexible work hours by letting workers use their device of choice—be it a smartphone, tablet or laptop—any time, from anywhere.

Yet BYOD presents significant security challenges to IT departments that are being called upon to support employees who want to use consumer devices for work. Protecting the corporate network from unauthorized access and rogue applications, as well as from malware and the loss or theft of confidential corporate data, becomes much more complex when these personal devices are allowed onto the network. Granting access to corporate data from these devices can also pose compliance issues for companies that operate under federal or industry regulations and guidelines.

While employees now expect the same user experience and level of access to corporate data when working with consumer devices as they enjoy with office-based PCs, IT must find ways to control this access so that these devices don't introduce new threats, impact compliance, put data at risk or monopolize bandwidth.

The challenges that IT departments face regarding BYOD aren't simply technological, however. While most IT departments are dedicated to enabling employees by supporting the devices they want to use to achieve their goals, there's also the sentiment that IT no longer sets the strategy. According to the *Computerworld* survey, 66 percent of respondents said that IT departments are losing control over the management and support of the multiple devices and platforms being introduced into the corporate computing environment, while 54 percent said that users now dictate to IT departments and vendors the technologies they want to use.

A NEW APPROACH

As the survey demonstrates, security is the No. 1 challenge posed by the BYOD trend, with 81 percent of participants responding as such. If IT departments can adopt solutions to the security challenges of BYOD so that corporate networks are protected, they can also start to regain some control over how, when and to what extent employees leverage these devices for work. This requires a new approach to securing mobile devices.

"BYOD actually turns things inside out—IT has less control over the device itself, so it has to rely on other measures, such as at the interface to the network," says Mark Bouchard, founder and principal consultant with AimPoint Group LLC. "Also, IT needs to be able to say, based on who is requesting access and the integrity of their device, whether that person should have access to certain resources or they should be blocked." Because IT often doesn't own the consumer devices that employees want to use for work purposes, many traditional methods of protecting endpoints can't be applied. For example, an enterprise may use an anti-virus or anti-malware program on all of the Windows desktops that it issues to employees; these packages typically feature some automation and therefore are straightforward to install, run and manage for IT. However, today's many different types of consumer devices run a handful of operating systems, so installing, managing and supporting client security software becomes nearly impossible.

Adding to the complexity is a new trend within the trend. According to the *Computerworld* study, 14 percent of respondents at large organizations and 11 percent of those at smaller ones said their companies are offering employees allowances to buy personal devices that can be used for work. This wrinkle to the BYOD trend brings into question what kind of applications can be used and what data can be stored on the device—strictly enterprise, or personal as well? It also further complicates security strategies.

ENABLE AND CONTROL

Given IT's limited control over many of the consumer devices employees are using today, the best strategy for securing these endpoints is to control the security of the device when it's connected to the LAN, both inside and outside of the network.

Ideally, securing personally owned devices on the corporate network means that IT gains control by dictating which data and applications remote users can access, based on the following:

- ✓ What device they are using and where they are logging on from;
- ✓ Limiting the applications used and Web sites accessed by the remote devices to the same applications and sites accessible to company-issued systems;
- ✓ Reducing the potential for consumer devices to introduce malware into the network.

Hear Patrick Sweeney, VP Product Manager, of SonicWALL talk about SonicWALL Mobile Connect.

Specifically, with the right security solutions, IT departments have the ability to extend existing polices or establish new ones that determine which corporate resources employees can have access to when logging onto the network from a company-issued device, and limit that access when employees are using personal devices. IT can also scan all traffic coming from employees using mobile devices—company issued or not—by implementing deep-packet inspection at the enterprise firewall. And while IT may not be able to control the consumer devices accessing the network, endpoint control policies can be established that perform user authentication and interrogation to determine if, for example, a device has been jailbroken and therefore must be quarantined or the connection rejected.

See how the Merial case study is great proof point for people accessing network resources from different devices.

"Such measures ensure integrity, so network administrators can feel confident that the network has not been compromised by the end user," says Matt Dieckman, product manager with SonicWALL.
To achieve high levels of enterprise security while enabling the use of consumer devices, IT managers should consider the following components:

- ✓ Support for a wide range of device types that run different OSes, including Windows®, Mac, iOS, Android™ and others.
- ✓ The ability for the IT department to determine the integrity of the endpoint device requesting access—for example, whether the device has been jailbroken—and grant different access levels, or reject the request, based on that determination. Such integrity checks should be performed each time a device-based user attempts to log on based on a set of predefined policies.
- ✓ Deep-packet inspection into traffic between the remote device and the network to scan every packet of data for malware.
- ✓ Application intelligence and control that gives the IT department visibility into the devices being used and the applications installed on them. Such visibility not only alerts to rogue applications that may carry malware that could infect the network, but also ensures that general-use policies to establish which types of applications may or may not be used in a corporate setting are extended to remote devices.
- ✓ Managed bandwidth of applications that don't fit the mission-critical criteria. For example, remote users connecting to the network and viewing bandwidth-intensive video can be throttled back so that business-critical processes aren't negatively affected.
- ✓ Implementation of corporate policies for Web browsing so that employees operate under the same guidelines whether in the office or remote.
- ✓ Wireless network options that allow IT administrators to establish a virtual LAN off of the wireless network that enforces a higher level of security for consumer devices.

CONCLUSION

While BYOD brings with it a number of new challenges for IT departments, the trend is likely to continue regardless of the headaches it introduces. As the consumer world grows more technologically advanced and people gain a greater understanding of— and preference for—consumer devices, these devices will become more prevelant in the corporate world. Employees and executives alike are voicing their opinions about the devices they want to use for work; IT is faced with having to establish BYOD strategies to meet these demands or suffer the consequences of these devices being used without IT's knowledge or approval. The BYOD trend gives IT departments the opportunity to better understand the company's business processes as well as employee preferences and work habits, and to develop mobility programs that meet employee demands without sacrificing security or compliance.

Having the right security measures in place to safely enable the use of personal devices while also minimizing risk is an important first step.

"The BYOD trend is being forced upon IT. Some departments are saying 'No, we can't support it,' or 'Yes, we can support it but there are caveats—we have to limit access based on the controls we put in place,'" says AimPoint Group's Bouchard. "At the end of the day, if the right solutions are put in place, IT can completely and in a straightforward manner support this trend. That means keeping users happy, boosting productivity and cutting support and equipment costs." «

CASE STUDY

OUR KIDS

Our Kids of Miami-Dade/Monroe, Inc. is the non-profit lead agency for community-based care in Miami and the Florida Keys. Since 2005, the agency has provided foster care, adoptions and related services for more than 3,500 abused, abandoned and neglected children and their families. As a contractor with the State of Florida, Our Kids receives state and federal funding. The agency employs approximately 200 personnel and works with over 1,000 community providers who require different levels of access to their database.

"We provide a safe haven and are responsible for the welfare of children that have been abused physically, sexually, or emotionally. We also provide care for children who have been neglected or abandoned by their birth parents," said Patricia Smith, chief information officer at Our Kids.

THE CHALLENGE: Ensuring appropriate levels of access to confidential data for remote workers

Our Kids acts as an umbrella organization within the community, working with hundreds of organizations that provide everything from psychiatric services, temporary shelter, schooling, medical care and services for teens transitioning into adulthood.

"Our real challenge was to safely and securely provide the right level of access to the right person," acknowledged Smith. "Not only did we want to introduce more mobile technology, but we wanted to make it much easier for case workers who work remotely."

At the same time, the agency's case management applications contain extremely confidential data, including birth documents, Social Security numbers and personal health information (PHI).

Our Kids was dissatisfied with the agency's previous remote access solution and firewalls from Juniper Networks®.

"We had users coming in through an SSL protected web portal, but once they got in, they were given role-based security in an application," reported Smith. "Unfortunately, we had inadequate logging. We could not restrict what data they were able to get to, so it was an all-or-nothing access level."

Additionally, the agency found that management of their previous Juniper firewalls was cumbersome.

"Managing Juniper was a time-consuming process: I had to manually update signature files for anti-virus or intrusion prevention services. The SonicWALL firewall is like a living entity: it updates itself," noted Jeff Koonce, IT infrastructure manager at Our Kids.

THE SOLUTION: Next-generation firewall with secure remote access and wireless functionality

Our Kids deployed a SonicWALL® E-Class Network Security Appliance (NSA) E7500 solution at its headquarters, as well as three NSA E6500 appliances at remote site locations and 16 SonicPoint-N wireless access points.

"SonicWALL offered us a cost-effective solution to provide safe and secure access to our community of users," said Koonce. "It became important for us to introduce a next-generation firewall with application intelligence into our environment and we specifically chose the NSA E7500 for its wireless and application intelligence capabilities, which we could not get from our Juniper firewall."

Combining SonicWALL Reassembly-Free Deep Packet Inspection® (RFDPI) technology with a multi-core platform, the SonicWALL E-Class Series is configurable to analyze and control thousands of unique applications.

"Deployment was straightforward," asserted Koonce. "It took me only 15 minutes to get the E7500 up and running out of the box."

To provide dedicated secure remote access, the agency deployed a SonicWALL Aventail® E-Class Secure Remote Access (SRA) EX7000 appliance. The SRA EX7000 offers an easy-to-manage clientless secure remote access solution for mobile enterprises with up to 5,000 concurrent users.

"We configured multiple realms that allow both internal employees and consultants to get to Our Kids' database," stated Koonce. "SonicWALL's End Point Control first checks if the end user's device is running anti-virus software, and if not, they are not allowed to connect."

The agency also chose to deploy SonicWALL SonicPoint access points on multiple frequencies. SonicWALL SonicPoint-N Dual-Radio integrates enforced 802.11a/b/g/n management across 2.4 GHz and 5 GHz

"CIOs can no longer fully control what devices access the network and who is using them. SonicWALL gives us a secure platform for future innovation, by letting our users connect using their own devices, while letting us offer new solutions at the same time."

—Patricia Smith, CIO, Our Kids

OUR KIDS CASE STUDY *continued*

bands at a combined throughput of up to 600 Mbps, for greater security and productivity.

"SonicPoints let us create separate entry points for Blackberries and iPhones, segregate traffic, and seamlessly monitor who is using what type of device from a central dashboard," said Koonce.

THE RESULT: Increased remote access with no added overhead, WLAN capabilities and application intelligence, control and visualization

After deploying the EX7000, we had a 30% increase in utilization of our network, with no addition to staff or changes to policies or procedures, or any other overhead," affirmed Smith. "Our user base has extended from 200 employees to a community of over 1,000—guardians, counselors, attorneys. We are even in the process of opening it up to doctors."

The SRA E7500 has given the agency application intelligence and control with real-time visualization.

"The visualization feature is excellent," declared Koonce. "I can look at one screen and immediately see which applications are being utilized the most within the network. Right off the bat, it showed us an unauthorized P2P program running on the network, which I was not able to see before with Juniper."

Koonce has used the solution to prioritize bandwidth for key applications, while restricting bandwidth for applications that are non-business related, such as streaming video web sites.

"Where SonicWALL really stands out is in separating traffic at the application as well as the network level," cited Koonce. "SonicWALL lets us use Facebook® to stay in touch with chronic runaways, while blocking the use of Facebook games for staff."

The solution has helped the agency retain its position as a technology leader in its field. "CIOs can no longer fully control what devices access the network and who is using them," asserted Smith. "SonicWALL gives us a secure platform for future innovation, by letting our users connect using their own devices, while allowing us to offer new solutions at the same time." «

CASE STUDY

TUSKEGEE UNIVERSITY

TUSKEGEE UNIVERSITY

Founded in 1881, Tuskegee University has approximately 3,200 students and 1,100 faculty and support personnel. Located 40 miles east of Montgomery, Alabama, the physical facilities of the campus include more than 100 major buildings and structures. The university maintains separate student and administrative networks. Recently, Tuskegee University implemented a SonicWALL E-Class Network Security Appliance (NSA) solution to costeffectively increase security, enable cross-platform mobility, streamline management and boost network performance and productivity.

THE CHALLENGE: Balancing protection with performance

Previously, the university ran Check Point® firewall software on a 3Com Crossbeam® system. Tuskegee's network repels up to one million malware and phishing attacks a week, which overwhelmed its firewall's capabilities.

"It brought our network to a crawl," said Fred Judkins, chief information officer at Tuskegee University. "The firewall could not handle the threats and volume of traffic."

The hit on performance affected both faculty and students.

"Educators could not download class materials because the firewall would take too long," said Judkins.

The problem was compounded by weekly software updates to 1,100 lab computers, as well as the increasing propagation of personal mobile devices among students.

"Each of our 3,200 students might typically use a laptop, desktop, tablet, smartphone and gaming console, with each device running multiple connections to the Internet," said Judkins. "If students cannot get the throughput to do what they want, they consider applying to other colleges where they can."

The old firewall was also difficult for the university to support and maintain.

"It would take 10 minutes to push out one simple change to an IP address," said Judkins. "We cannot wait that long. If we have a zero-day attack, we need to update instantaneously. Plus, it was a nightmare installing SSL VPN licenses with Check Point."

Working with CDW-G, Judkins considered replacement solutions from Barracuda®, Fortinet®, and Check Point before finally selecting SonicWALL.

TUSKEGEE UNIVERSITY CASE STUDY *continued*

> "SonicWALL lets our users easily connect from their iPads® over SSL VPN," said Judkins. "Our executive staff uses it. One member said it was like sitting at his desk."
>
> —Fred Judkins, CIO, Tuskegee University

"Barracuda was just not there yet on next-generation firewall capabilities. And Fortinet was unrealistically expensive. We expected Check Point to have a high-performance next-generation firewall, but SonicWALL beat them hands down. On the same peak-time connection tests, throughput with Check Point was only 7 MB, while with SonicWALL it was up to 90 MB. It just rocked," said Judkins.

Service was another selling point for Judkins.

"SonicWALL technicians were very fast and professional," said Judkins. "We decided to add SonicWALL Platinum support, which was very economical compared to what we were paying for with Check Point support."

THE SOLUTION: SonicWALL E-Class NSA E7500 with Mobile Connect

The university deployed dual SonicWALL E-Class NSA E7500 Next-Generation Firewalls paired in High Availability (HA) mode.

"We activated a number of features, including anti-malware, anti-spam, application intelligence and control, as well as SSL VPN," said Judkins.

The NSA E7500 combines SonicWALL Reassembly-Free Deep Packet Inspection (RFDPI) technology with a multi-core platform. It is configurable to analyze and control thousands of unique applications, whether unencrypted or encrypted with SSL.

"SonicWALL lets our users easily connect from their iPads® over SSL VPN," said Judkins. "Our executive staff uses it. One member said it was like sitting at his desk. Instructors can post grades and access the resources they need. It works great. We can get Android® devices connected as well."

The SonicWALL Mobile Connect™ unified client app for iOS provides iPad, iPhone®, and iPod touch® users full access to network resources over encrypted SSL VPN connections to ensure confidentiality and data integrity for users outside the network perimeter. Deployed on or with a SonicWALL Next-Generation Firewall, Mobile Connect enables Clean VPN to remove malware from communications relayed through iOS devices.

THE RESULT: Easy, high-performance security with greater ROI

SonicWALL saves us up to $100,000 per year by consolidating network and mail filtering on the firewall," said Judkins. "We did not have to upgrade multiple outdated and expensive point solutions. Because it is all in one package, it centralizes management of most of our security services in one place."

Judkins appreciates the solution's ease of use.

"We have the ability to remotely and granularly designate what firewalls users can get to, what rules they can change and what they can see," said Judkins. "Our university president can view network traffic in real time. We can set up automatic reports to be sent via email. If we lose our primary connectivity, it rolls over to a cellular connection. It is unbelievably fast and simple."

The NSA E7500 delivers the performance the university requires.

"Firewall services never exceed 10 percent, even at peak," said Judkins. "We can have 10 classrooms teleconferenced in high definition for distance learning, which was impossible with the old firewall." Next year, the university plans to upgrade to gigabyte connectivity.

"The E7500 will take it just fine. We can prioritize traffic allocation on the fly," said Judkins. "It even has the intelligence to differentiate whether a data packet is part of a music video or educational video. And it is graphical, so it is very easy to use." «

For more information about SonicWALL visit www.sonicwall.com