



Eye Centers Focus on HIPAA Compliance

A Case Study in Network Security

“Every location that had WebBlocker rolled out had the number of infections reduced significantly -- very near zero,” **Stephen Brown, IT Manager, Midwest Eye Consultants, P.C. (MWEC)**

BACKGROUND

Midwest Eye Consultants, PC (MWEC) operate 22 primary care offices, three surgical facilities, an optical lab, and a nursing home division throughout Indiana, offering optometry services, ophthalmological care, and eye surgeries. With such a widely distributed medical enterprise, connectivity and security are major concerns.

To address these concerns in a cost-effective and compliant manner, MWEC partnered with Intrasec Technologies, a long-established, diverse IT consultant and managed services provider from Northeast Indiana. Intrasec manages and monitors MWEC’s twenty servers along with their backups, and acts as a second line of support for the internal IT staff as well as taking on a strategic consulting role.

CHALLENGE

MWEC’s practice sizes are diverse, ranging from single-practitioner offices to fully staffed surgical centers. A central practice management system (CompuLink EyeCare Advantage) runs out of the corporate data center, over Citrix sessions, to handle scheduling, accounting and related business functions. Due to the fact that these records include confidential patient data, the company is subject to HIPAA regulations for data security and integrity.

There are more than 300 individual PCs to protect, at widespread locations, all requiring connectivity to the data center and posing a possible security concern. Web-surfing employees were a constant worry. “There had been a problem with pop ups and people clicking on things,” explains Stephen Brown, IT Manager. “We had a couple occurrences a month where people thought they were doing us a favor by installing an antivirus program, not realizing the program was malware. That created lots of headaches on the machine.” This created a situation in which a compromised PC became an attack vector that could put patient data at risk.

WATCHGUARD® SOLUTION

The WatchGuard WebBlocker service proved an ideal solution for handling the many small offices, as well as the users at corporate headquarters. According to Thomas Polk, Divisional Manager for Intrasect, “The biggest issue is that most of their remote sites are just a couple of workstations. Rather than manage web use through applications on each individual machine, the best approach was through a firewall VPN appliance on the edge.”

A WatchGuard Firebox X Peak™ 6500e was already in place protecting headquarters and the data center. Older WatchGuard units were handling the back-office VPNs at each practice. Thanks to WatchGuard’s liberal trade-up policy, replacing the existing units with new ones made more economic sense than enabling web blocking on the older units. Intrasect and MWEC installed new WatchGuard Firebox X Edge™ 20e or 55e devices at each of the satellite offices, with full UTM security subscription bundles, including WebBlocker.

BENEFITS

Immediately, the number of compromised machines dropped significantly. “Every location that had WebBlocker rolled out had the number of infections reduced significantly -- very near zero,” says Brown.

Hours Saved on Scrubbing Infections

Brown and MWEC cured more than the security headaches. He says, “I had to spend a few hours cleaning up the machine if the infection wasn’t bad, or else reinstall the system from scratch. Very rarely could I fix those problems remotely. So, I also saved anywhere from a half-hour to a 2-1/2 hour trip to get on site to correct the issue.” WebBlocker eliminated that time-consuming task, as well as the lost productivity from a workstation that was down.

The Most Cost-Effective Web Blocking Solution

For Polk, the WatchGuard solution was far and away the most cost-effective solution available. “The only other choice would have been to backhaul all the Web traffic through the data center and then back out to the Internet,” he says. “The problem is, that would have killed the bandwidth. There are already four T1s coming into the data center to handle the 200 terminal services sessions. If I were to put browsing on top of that, we would be moving to eight T1s. That’s really ineffective compared to upgrading to boxes with UTM bundles, managed from a central location.”

Developing the Web-blocking policies was, and continues to be, a balancing act says Polk. “You have to walk the line between screwing the system down to five allowed sites, which we can do, or to say, ‘We’re going to trust you to use your best judgment and be good employees.’ We’re doing basic, traditional content filtering in terms of sexual content... and some specifics, such as social networking sites. We don’t necessarily see a benefit to allowing them, at least at this point.” Polk is currently putting together a system for analyzing and reporting on the Web usage data pulled from the WatchGuard appliances, to further refine the policies.

Opening Business Opportunities in Small Communities

“This is rural Indiana, and there are lots of cornfields between here and there. We have people here still driving horse and buggy. This is flyover country,” declares Polk. That means that connecting sites and enforcing distributed security in a cost-effective manner is essential.

In fact, one element of MWEC’s business is purchasing independent, established small-town practices, allowing longtime practitioners to continue serving their patients while taking over the administrative burdens. Having the WatchGuard devices allows Midwest Eye to take advantage of these opportunities. Brown says, “Buying a leased line between Wabash and Chesterton would be a ridiculous expense. It wouldn't be economically reasonable to have an office there. The cost-effective way is to purchase business class Internet at the location, and use the WatchGuard product to provide point-to-point encrypted secure channels for us to operate over.”

ADDRESS:
505 Fifth Avenue South
Suite 500
Seattle, WA 98104

WEB:
www.watchguard.com

U.S. SALES:
1.800.734.9905

INTERNATIONAL SALES:
+1.206.613.0895

ABOUT WATCHGUARD

Since 1996, WatchGuard has been building award-winning unified threat management (UTM) network security solutions that combine firewall, VPN and security services to protect networks and the businesses they power. We recently launched the next generation: extensible threat management (XTM) solutions featuring reliable, all-in-one security, scaled and priced to meet the unique security needs of every enterprise. Our products are backed by 15000 partners representing WatchGuard in 120 countries. More than a half million signature red WatchGuard security appliances have already been deployed worldwide in industries including retail, education, and healthcare. WatchGuard is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America.

No express or implied warranties are provided for herein. All specifications are subject to change and any expected future products, features, or functionality will be provided on an if and when available basis. ©2009 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard logo, and Firebox are either trademarks or registered trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other trademarks and tradenames are the property of their respective owners. Part No. WGCE66625_091109