



Indiana Health Care System Safeguards Patient Information Via Award Winning 3Com®, TippingPoint™ Security Solution

The Challenge: At IU Medical Group - Primary Care (IUMG), caring for patients involves more than providing world-class health services. It also requires a healthy network – one safe from hackers, worms, and spyware that might compromise the performance of the organization's life-critical applications or confidentiality of its medical records, which would breach HIPAA regulations.

This level of security must extend to the organization's 24 clinics throughout central Indiana. Network security is also critical for the Indiana University-affiliated organization's claims administration and payment services, which ensure the region's hospitals and medical practices receive timely insurance reimbursements. It further extends to network connectivity IUMG provides to a local battered women shelter and a cache of local health and human services organizations to which it provides bandwidth. Equally important, IUMG must secure its vast network without incurring latencies in network performance.

Previously, however, IUMG's Cisco PIX 515 firewall did not provide comprehensive protection to IUMG's sites and the external agencies that share its bandwidth, making it impossible for IT staff to isolate and disinfect affected departments before the virus could spread. Furthermore, the IT department needed additional network drops to test new software and equipment before adding it to the network, but was housed in a building with concrete walls that made additional wiring prohibitively costly.

In order to safeguard its data and better control its network, IUMG sought a powerful, cost-effective security solution that would interoperate smoothly with its existing Cisco-based data infrastructure.

Why TippingPoint, a division of 3Com

At first, IUMG assumed it had to purchase standalone systems to address each specific network security need, such as virus protection, Denial of Service protection, intrusion prevention, and e-mail filtering. It soon discovered, though, that this patchwork approach was expensive and inadequate. For example, simply deploying anti-virus software on desktop machines costs thousands of dollars annually in licensing fees. Moreover, these systems only repair viruses after the infections disrupt the network. Also, IUMG could not require agencies sharing its bandwidth to implement them.

Accordingly, IUMG sought a more cost-effective, pervasive, and straightforward approach to network security. The healthcare organization found the combination of high performance and superior value it sought in a TippingPoint Intrusion Prevention System.

"We can now instantly block malicious traffic, music downloads and online gaming, preserving our bandwidth for legitimate, health-critical applications."

Brian Worrell
Network Manager
IUMG

“I had read about the TippingPoint IPS solution’s success at other large deployments, including hospitals,” said Brian Worrell, network manager, IUMG. “It is the only IPS to receive the coveted Gold Award from The NSS Group, the world-leading independent security testing facility, and Best Security Solution 2005 from SC Magazine.”

Lodged at Wishard Hospital, the standardsbased 3Com and TippingPoint solution interoperates seamlessly with three Cisco routers and a Cisco switch at IUMG’s LAN core in Wishard, which provides Internet and inter-site connections to all users. Using the TippingPoint Intrusion Prevention System, the medical group now meets all of its network security requirements in one fully integrated platform. What’s more, TippingPoint’s Digital Vaccine® service delivers new filters on an as needed, often daily, basis to maintain evergreen protection from the latest vulnerabilities, exploits, viruses, and rogue applications.

IUMG also relies on 20 3Com IntelliJack NJ200 in-wall switches, converting each of the individual Ethernet drops in its IT department to four fully managed ports.

The_Benefits

By investing in 3Com solutions, Indiana University Medical Group has gained complete network security and will save more than \$30,000 in software licensing fees and wiring costs in 2005 for an ROI of little more than one year. Most importantly, the TippingPoint solution ensures that the quality of IUMG’s care will not be disrupted or compromised via breaches in network security. It further enables IUMG to comply with the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA), which requires medical providers to protect patient privacy by preventing unauthorized persons from retrieving, viewing, changing, or destroying protected health information (PHI).

A powerful gatekeeper at IUMG’s Internet portal, the TippingPoint IPS accomplishes these objectives using a full arsenal of security features at a fraction of the cost of piecemeal systems.

In its first two weeks of operation, for example, TippingPoint prevented over 100 malicious attacks, ranging from sequel server attacks, Web server attacks, and DoS attacks. The robust capabilities of the TippingPoint IPS allow all incoming and outgoing Internet traffic on IUMG’s network to pass through a single Gigabit port. Another port monitors traffic to and from IUMG’s servers.

Together, these protected ports protect IUMG’s network from potentially debilitating attacks without any performance degradation. Two additional ports offer scalability and additional LAN protection. It also limits network access to authorized users and tracks bandwidth usage for better overall network performance. In addition, the TippingPoint IPS monitors Instant Messenger usage network-wide to guard against intrusion and monitor how much bandwidth it is using. If necessary, the TippingPoint solution can conserve bandwidth by blocking IM traffic. As a result, the network use is now more efficient and work-appropriate at every IUMG site.

“The only way to keep PHI secure is to know what people are doing on devices that contain it, and the TippingPoint solution gives us that capability,” explained Worrell. “We can now instantly block malicious traffic, music downloads and online gaming, preserving our bandwidth for legitimate, health-critical applications.” Adding to this value, the TippingPoint IPS monitors up to four Gigabit network ports with a single annual software license.

Although it is extremely powerful, the TippingPoint appliance’s intuitive graphical user interface makes the application remarkably simple to use and very scalable. The TippingPoint solution also offers comprehensive reporting of all securityrelated events for IUMG’s entire systems and for individual servers.

The fully managed IntelliJack NJ200 switch allows IUMG’s IT staff to set up multiple virtual LANs (VLANs) to test new equipment and software before adding it to the network, further protecting the organization’s data infrastructure and resources. When the organization’s corporate

office relocates in mid-2005, IT staff will easily move the IntelliJack systems to the new building, facilitating network access while reducing the cost of running additional cable – at \$200 per drop — by approximately \$12,000.

“TippingPoint and 3Com delivered a versatile, value-driven solution that is safeguarding our

computing environment and improving network performance,” Worrell concluded. “Additionally, with the TippingPoint Digital Vaccine service, we are safe today and tomorrow, leaving us better able to deliver quality healthcare now and in the future.”

“The only way to keep PHI secure is to know what people are doing on devices that contain it, and the TippingPoint solution gives us that capability.”

Brian Worrell
Network Manager
IUMG

Corporate_Headquarters: 7501B North Capital of Texas Hwy. > Austin, Texas 78731 USA > +1 512 681 8000 > +1 888 TRUE IPS

European_Headquarters: Herengracht 466, 2nd Floor > 1017 CA Amsterdam, The Netherlands > +31 20 521 0450

Asia_Pacific_Headquarters: 47 Scotts Road #11-03 Goldbell Towers > Singapore 228233 > +65 6213 5999