

Wellstar Health System

Deploys TippingPoint as “Best Practice” for Regulatory Compliance to Protect Electronic Medical Records, Patient Data and Corporate Assets

CASE STUDY — WELLSTAR



The Challenge: When Corporate Compliance Information Security started planning for WellStar Health System’s HIPAA compliance program, they took the requirement to meet best practices in information security seriously. While other health organizations often tried to paper over their security vulnerabilities, WellStar implemented a sophisticated and comprehensive, technology-based security blanket to ensure that patient data stays confidential. The most active and important element in that security program is an intrusion prevention system that automatically blocks attacks, sometimes even before the attacks have been reported by security experts.

“TippingPoint stops spyware from being installed, blocking several hundred spyware attacks each day. What’s great about it is that it also blocks outgoing traffic attempting to reach the spyware data collection sites. There’s a huge amount of spyware on the Internet and it is a compliance issue as well as a performance issue.”

Bonnie Norman
Wellstar Health System

What led Wellstar to decide to upgrade your security infrastructure? Did you experience a major attack?

It was not an attack. HIPAA was the reason that the security upgrades were planned and funded.

Before HIPAA, how did you control malicious traffic?

We had a policy of locking everything down at the firewall. Any physician or other person who needed to allow traffic to be accepted had to justify the change.

Was that sufficient?

The problem with firewalls is that they are too broad - you have to block entire categories of traffic. You would have to block all Web traffic to stop Port 80 attacks. That isn’t good enough.

How did you determine what security technologies were needed for best practice?

Reading the HIPAA legislation, we realized that we needed to implement best practices. We reviewed the NIST guidelines that HIPAA recommends, and we also asked two questions: “What are the best practices?” and “If we were a bank, what would we be doing to protect our assets?”

The Solution

WellStar determined quickly that following best practices meant that they needed an IPS solution to provide automated threat protection for their network and the critical data stored within their network. WellStar thoroughly tested the four leading IPS solutions and selected the TippingPoint solution as it was the best on every one of their selection criteria. WellStar now uses the TippingPoint IPS solution to protect their public connections to the Internet, connections to other external parties, all connections to their data center, and to protect and isolate each subnet on their network.

What types of tools did you include in your portfolio technologies to protect your patient information?

We already had a firewall and had ISS’s Internet Scanner for vulnerability scanning. We added an intellectual property leakage detector, an IP traffic

recorder so we could be certain of what had and had not happened on our network, and a node analyzer and compliance tool that told us what was and was not installed on each of our systems. We also set up a system to ensure that laptops and other computers get regular virus updates. But our best purchase was an intrusion prevention system.

Why was intrusion prevention best?

Because most of the things the other security tools do we could have done with a sniffer and some programming. But there’s no way any user organization has the time to keep ahead of all of the new vulnerabilities and continually write and test detectors that will find malicious traffic and stop it without blocking traffic we need.

How did you know that you needed an intrusion prevention system?

The main reason was what we learned from the SANS Hacker Tools and Incident Handling class. It showed us the tools the hackers are using and how they get around the standard defenses that we and other organizations were using. When I realized this, I wanted to throw up in a corner. I knew right then that we needed to find some way to block the more sophisticated attacks. There was no way we could claim to be using best practices without intrusion prevention.

Do other hospitals also see intrusion prevention as a required tool for HIPAA compliance?

The smarter ones do. WellStar participates in the Atlanta Health Care Security Council, consisting of security and privacy officers from all the hospitals in the area. We learn from each other. I think most hospitals recognize that the law demands best practices.

What steps did you go through to find the right intrusion prevention system?

We started in January 2004 and had a target of purchasing by June 1. We looked at four leading products and tested each one, in house, for 30 days.

As you went through that process, what selection criteria did you decide were most important?

We had six key criteria: (1) References - how

TippingPoint®

TippingPoint Case Study — Wellstar Health System

satisfied the customers were, (2) Ease of Use, (3) Fast Deployment, (4) Consistency - Is what I see what is truly happening? Or in other words, no false positives, (5) Fail open - the device needed to allow the unfiltered network traffic to stream into our network if it failed. If a device fails closed all network traffic stops. We needed a device that allowed care to continue and alert us that it had failed, and (6) Zero or low latency - it was important to us that the device had little or no impact on our network traffic.

Which one did the best job of meeting your six criteria?

TippingPoint was the hands-down winner. It did better on all our criteria. As we analyzed other products, they fell out of competition for one or more of the following reasons: (1) They were not appliances and we wanted an appliance for ease of use; (2) They were hard to install and even harder to learn. They had to be modified and tuned to watch our traffic. TippingPoint just worked; (3) Out-of-the-box they didn't seem to have knowledge of what bad traffic was. They seemed to need to learn from our traffic; (4) The references we called told us that they had to spend too much time watching and managing the boxes. They also didn't explain the update process very well. (5) The devices could only be configured to fail closed; and (6) There was a significant difference in our network traffic.

How many segments did you protect and how many IPS systems did that require?

We are using two TippingPoint IPS appliances. We set it up so that it protects us where we are connected to the outside and to our server farm. It currently protects all points of access to external traffic and is being deployed with the use of routers to protect traffic among each of our subnets so an infection on one subnet won't get loose and hurt computers on other subnets.

What was your deployment strategy?

We deployed in a cascading plan from July through October. An IPS is an in-line device, which meant that we had to bring components down while the installation took place. To avoid any major impact on operations, we deployed on each segment when the segment had planned downtime for router or server upgrade or other change management tasks. When we first installed the TippingPoint IPS, we took all the suggested filters and turned them on in monitor mode for 30 days. We watched what would have been blocked, and got alerts, but we didn't block anything. During our initial implementation period we found no false positives. After 30 days we implemented all recommended filters. Then we started turning on other filters, like instant messaging. We added about 10 filters a day for 45 to 60 days. A few people complained.

Can you give us an example?

When we started filtering anonymous FTP, a few people complained because one or two applications used it between internal servers. They were trying to do midnight transfers and TippingPoint stopped the transfers. So we adjusted the filter, not to allow anonymous FTP in general, but to allow it point to point, from IP address to IP address, and from port to port. And TippingPoint provides all that capability.

Do people try to go around the instant messaging filters?

About five times a week, someone will install one of the large Internet offered IM products (IM, AIM, Yahoo Messenger, etc.), and we block it. It is our policy that we will not allow instant messaging or other ISP software on employee desktops.

How can you be sure it actually works, that it is actually blocking attacks?

It keeps a log of all the attacks it is blocking, and a dashboard that gives me a quick heads up overview of the ongoing events. Many we never would have known about until after they took our systems over. Some of the attacks try to float in on a Web page and take over a computer; TippingPoint blocks them. Others come in as exploited ping packets on ICMP_ECHO traffic. That's a good example of why firewalls don't work well enough. You cannot block all requests because some are essential for Internet operations. You can work around not allowing pings through your firewall but internally we can't operate without allowing them. Without TippingPoint, we would not have a defense against the ICMP_ECHO attacks. Frequently when I get a notice of a new attack, I'll look at the logs and find TippingPoint is already blocking that attack. We talked before about instant messaging. Some of them try to morph from port to port. TippingPoint blocks them all because it knows what instant message traffic looks like inside the packets.

What did you do when users complained about traffic you are blocking?

We get no pushback. We want to ensure that we provide all of the tools available for our teams to provide world class healthcare. Whenever someone complains, we say, come with us and help us explain why you need it to the executives on the "Information Compliance Management Committee." We offer to help them develop and give the presentation. Few of them proceed with requesting an exception to or modification of the security policies and procedures from the Information Compliance Management Committee.

How much of your time does it take to support IPS using TippingPoint?

I look at the dashboard three or four times a day. Dashboard review usually results in log research about once a day. Once every two weeks I see an event that takes more time. For example the Loki ICMP_ECHO packet exploit we talked about before that can be used as a backdoor into a system by providing a covert method of getting commands executed on a target machine. The Loki exploit can be used as a way of clandestinely obtaining information off of a target machine or it can be used as a covert method of covert communications between users. That took more time. We had an outbreak that initiated from a laptop that had been used offsite and introduced back into the network. It propagated the threat on the home segment of the device quickly and took us about three man days to contain and eradicate. Another example of something that takes time was .zip attachments. We told people they could be used only for clinical data, but TippingPoint showed us that people were working around that rule. So we expanded the policy. And that took some time. Now we log and review zip attachments and block zip attachments with

potentially dangerous files inside with .EXE, or any other potentially threatening file type extension.

How good was technical support when you needed help?

We don't need very much help because it works so well, but at the very beginning we had trouble with the first patch. We couldn't get it to install on the server. In less than two hours, TippingPoint had someone on the phone, who walked us through it. Now patches come through and they are applied automatically with our approval.

What do you like best about the service?

Every single vaccine (filter) they send us tells what it is going to log, alert, or block in an understandable paragraph. It tells why you would care and what it might affect and what it will or will not block. It's just great. That's another area where TippingPoint was much better than the other products we evaluated.

Was there anything else TippingPoint does for you that you didn't expect?

Yes. When we bought the systems, we didn't know they were adding spyware filtering. TippingPoint stops spyware from being installed, blocking several hundred spyware attacks each day. What's great about it is that it also blocks outgoing traffic attempting to reach the spyware data collection sites. That means if the spyware got on a laptop while the laptop was at someone's home or at a hotel while the person was on travel, TippingPoint still stops the data from leaving our organization. There's a huge amount of spyware on the Internet and it is a compliance issue as well as a performance issue.

How is spyware a HIPAA compliance issue?

Spyware collects information and sends it out. It steals e-mail addresses, Web activity, the full contents of cookies. That might not matter much at home, but on a healthcare desktop, it becomes a compliance issue.

Anything else you can think of that it does for you?

Our Director of Networking Services is looking for help in traffic shaping. That's a capability that allows us to limit traffic to some of our sites where they are consuming a lot of bandwidth for personal activities, i.e. watching stock tickers or shopping, and to use that bandwidth where it is needed most for healthcare. TippingPoint's appliances provide that service.

What's the bottom line?

The results of WellStar's successful deployment of the TippingPoint IPS solution included (1) support of their compliance program as the IPS solution fulfilled their security best practice requirement, (2) a significant decrease in spyware as WellStar found that the IPS blocked daily spyware downloads and out-bound transmissions to spyware data collection sites, (3) automatic prevention of IM application use as their security policy prohibits the use and installation of IM programs, (4) protection from dangerous .zip file downloads, which can hide potentially threatening executable files, and protection of patient medical information.

Corporate Headquarters:

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

European Headquarters:

World Trade Centre Amsterdam
Zuidplein 36, H-Toren
1077XV Amsterdam
The Netherlands
+31 20 799 7629

Asia Pacific Headquarters:

30, Cecil Street, #18-01
Prudential Tower
Singapore 049712
+65 6213 5999