

About St. Joseph's Health Care

St. Joseph Hospital is southern New Hampshire's largest acute care hospital and trauma center. We are dedicated to providing innovative, high quality health care in an environment of dignity, compassion and safety. Our patients and families benefit from the region's most experienced Breast Care Center and most comprehensive Cardiovascular Center. The Oncology Center offers clinical trials through a collaboration with Dana-Farber/Partners CancerCare. Our Rehabilitation Center is a CARF accredited, 24-bed specialty unit offering personalized care for patients recovering from stroke, head trauma, amputation, and joint replacement surgery. Our new \$25 million ambulatory care building, which opened in January 2006, expands our leading-edge services in the Cardiovascular Center, The Oncology Center, the Endoscopy Suite, the SurgiCenter, The Roger Dionne Senior Center and the Emergency Department.

About Ian Burke

Ian Burke, GCIH, MCSE, is the data security administrator at St. Joseph's Health Care. He focuses on monitoring, administering security, security education and security policy.

SANS Summary

The CIO asked his new data security administrator to identify top security priorities for St. Joseph's Health Care. Feeling that a well orchestrated firewall wasn't enough of a defense, the admin chose an IPS to highlight the traffic moving in and out of the hospital network. His theory: "If we don't know what's coming through the front door, we're not going to be able to protect ourselves." The solution he chose offered great insight into the network traffic and fantastic technical support.

~~~~~

## Interview

Q. Can you describe your network?

A. We have about 1,200 PCs, 100 odd servers, so mid size; about 2,000 users. We have the Physician's Portal, where they can pull up things like x-rays and lab results and charts, but we restrict their access. They can get it from their homes, they can get it from our network but we don't have a fully wireless network so they're not walking around with BlackBerrys and they also cannot chart from that application or enter physician information. We're headed that way; we're not totally paperless, but we're probably let's say, 60 - 70 % of the way there.

*\* To hear Ian Burke expand on his answers, view his presentation slides, and listen to his answers to many more detailed questions asked by other users from around the world, go to <http://www.sans.org/webcasts/archive.php>.*

Q. What kinds of issues do you think that's going to bring as you move to 100%?

A. From a security standpoint, I'm concerned about data integrity. I know our application people need to be worrying about that, but I still worry and I still ask questions like, do we have data integrity checks? I also worry about what sort of security bounds we have in place because our security vendor is not super security-centric. We have a fairly homogenous network here as far as vendors are concerned, so when you have a problem with an application chances are pretty good you're going to have the same problem with every other application. We see a lot of the same problems throughout our network.

Q. Does NitroSecurity play any kind of role with HIPAA?

"I needed something more robust for the edge that would give me the information that I want and can report in a timely fashion."

A. Our use of NitroSecurity is growing, but our primary use is as an edge appliance. There's a role for HIPAA in that we use them to try to protect things going in and out of the edge of our network, but from a policy standpoint we really cover our HIPAA requirements in that we say no PHI goes out within our network. We recently upgraded from Nitro's ESS appliance to Nitro's ESM appliance. We're integrating SNORT boxes throughout our network into Nitro's ESM appliance to give us a better view of the traffic across our network and correlate it to get a better view of the whole

picture. This lets us handle how that data travels from one server to the next or from one client to a server and if we have an inconsistency in those servers or in that client server communication, I can see it better with this appliance.

Q. What was the problem that you were having at St. Joe's that prompted you to look for this product?

A. When I was hired I came into a brand new position. My CIO said, "I want you to interview the people in the department and put together the priority list." I interviewed everybody in the department and put together their top priorities and then added in my top priorities as well. One of the things I knew was really important was intrusion prevention, which they didn't have. So I brought that in as a priority.

Q. And when you decided to do this, did they automatically approve the budget for it? Did you have to justify it six ways from Sunday?

A. I came in half way through the year and there was no budget approved for my position for the rest of that year. There was a budget project approved for network access control and I came in and said, "Look, we need to do this." And they said, "Well, we have no money." So I said we're going to put in SNORT boxes and we'll just make that work. And then we'll expand it from there to this--I ended up stealing the money from the network access control project because I convinced them that this was more important than

network access control and I still believe that it was. Both are really important but I think that if you don't know what's coming into your network then it doesn't matter what's on your network.

I got the SNORT boxes up and running on the network and that gave us an image of what was here, at least a start. And then we went out and started looking at different IPS solutions and moved forward from there. And then, yes, I justified it six ways from Sunday and convinced them that they needed to give me that money.

Q. What did you use in your argument to them for the money?

A. I said we had a collection of different issues that were identified and that if we don't know what's coming through the front door, we're not going to be able to protect ourselves. And though we had an excellent firewall solution, we didn't have that next step behind it. They liked the SNORT solution because of the price tag but examples of how a commercial solution would be able to give us reporting and more live data really made it worthwhile.

Q. Which pieces of what it found were most persuasive? What among the things that the SNORT boxes reported to you were the ones that seemed to resonate more with the people who had to say, "Yeah, we have to do something about that."

A. We have a fairly quiet network. We picked up a lot of traffic in the off hours, people going out to commercial sites that they shouldn't and other things like that, and we also picked up some HTTP traffic coming in.

Q. Did any of it get senior management to say, "Oh, we've got to stop that, what do we need to do?" Or was it just the sum of it?

"NitroSecurity's interface is absolutely one of a kind."

A. It was the sheer volume of it. The SNORT box had so much data it was almost unmanageable. And there were things in there that we needed to track down—and SNORT is a little bit cryptic. I was getting literally thousands and thousands of hits and those boxes were predominantly internal. So I wasn't seeing a lot of data going in and out of the hospital. It was between servers.

Q. So you were able to say, "Look, we've got all this stuff going on, some of it I can figure out, some of it I can't. I need a better tool to figure out which of these things are really problems."

A. Right. And the big thing I was able to say, "If this is on the inside, can you imagine what's going on at our edge? We need a commercial tool that gives us better reporting, better processing power." I had so much data that my little PCs that were built up on old retired boxes just kept dying. I said I needed something more robust that I can put on the

edge that will give us the information that we want, that can report in a more timely fashion.

Q. And they went along with it because you showed them that a lot of stuff was happening?

A. Right.

Q. What other tools did you consider?

A. Sourcefire. Nitro. Cisco and we looked at one or two others. We found that Nitro is very matter of fact, in your face, here are the numbers. With just a couple of clicks you're at the packet level if you want to be there. You can have alerts in bar graphs in numbers. First IP destination, IP port number and alert ID.

Q. The other guys kind of hide that from you by thinking that you're not that smart so you shouldn't want to have all that detail.

A. That's the way it felt. They treated it as more of an executive tool. Cisco is one we really spent a lot of time with because we're very much a Cisco shop and our network administrator really liked the idea of taking it from the Cisco side. We liked it because we had AC5520s for our firewall and we could just plug in the Cisco IPS.

**"If we don't know what's coming through the front door, we're not going to be able to protect ourselves."**

Q. Right so it was a big decision not to do that.

A. It was a huge decision.

Q. It didn't hide the detail from you?

A. Right now I can analyze all my alerts from a 24 hour period in about 30 minutes. To do that on a Cisco Mars I'm guessing would take me about four or five hours.

Q. Because the digging for the detail isn't obvious and isn't easy and isn't quick?

A. Right. It's buried. I'm guessing you'd figure out a way to streamline it on the monitors but from what they were able to show me, it's a totally different beast and they could never show me how to do what I do now.

Q. Does everybody who works at Nitro know how to do that?

A. I think so. I mean you very quickly go from the sales staff to the engineers and to the development team and they all work very closely together but I don't know if all the salespeople know how to do it.

Q. And you always had access to the sort of stuff that you did need?

A. I'm now working with a salesperson named Craig Carter and it is almost impossible to get in touch with him. I mean I can call him 10 times in a week and not hear back from him. So what I end up doing is I just call Bob, who's the engineer I work with and he'll fix

the problem or hook me up with Craig. If I've got a sales question it's almost impossible to get in touch with the sales team. That's my biggest complaint about Nitro now, is that their sales staff, I don't know if they're just short staffed or what, but it's hard to get in touch with them.

Q. Interesting. Mostly you would have had that complaint about the technical staff but here it's the sales guy.

A. And technical staff is awesome. My support contract is from 8:00 a.m. to 5:00 p.m. Eastern Standard Time and I have called their support staff at five o'clock in the morning and they pick up the phone and they talk to me. And then I'll get a call later from a sales guy saying, "Hey, you can't do that." That's how to get in touch with the sales guy.

Their technical team is incredible. They're easy to get in touch with, you call them and they answer the phone. If they're busy they call back within an hour and if they're busy and they can't call me back their local engineer will call me--if he can't get to me on the phone, he shows up at my door. Their technical team is phenomenal.

Q. How was implementation? What did it take to get it operational? How long did it take to get one in? Did they send you a sample unit or did you order it and they brought it?

A. That was actually another selling point for Nitro. We had a hard time getting Cisco out here to give a demo. And we took a look at Sourcefire; we weren't impressed with it.

Q. And since you're a SNORT shop I would have expected you to be impressed with it. So that's a little bit confusing. What was it that wasn't there?

A. Their interface. It seemed backwards. It was very confusing to navigate through their product. Once you got there it was nice. And it was confusing so we just said we weren't interested. After our first demo with it we agreed this was not the product for us and we just walked away from it.

"We had the NitroSecurity demo up and running in about three hours."

Q. That's the first I've ever heard that.

A. So that was a pretty quick and easy decision for us. I was surprised too, being a SNORT shop I thought I would like it. But the SNORT piece was easily decided for us because Nitro is almost entirely SNORT rule based.

Q. So you have all the benefit of Sourcefire but with a better interface. Now getting it in, getting the box in, again how long did it take? It came in overnight and you plugged it in and . . . ?

A. We had the demo up and running in about three hours.

"Nitro has an amazing database that allows it to correlate the data and transfer it and look at it faster than anything else I've seen."

Q. Was there any difficulty in tapping in to the right spots?

A. No, we have a downtime on the first and third Wednesday of every month from about four in the morning until about six in the morning and they showed up, at four in the morning with the demo boxes and big smile on his face, and we put the Nitro box in. We had figured out where we were going to put it, just plugged it in and he had it preconfigured. We plugged in the IP addresses because we had those and it was up and running. We went downstairs and

plugged in the ESS and configured it and it was up and running and then he spent about an hour or so with me setting up some rules and showing me how to navigate through it.

Q. Did you use it only in monitor mode at the beginning?

A. Yes we did. We just played with it.

Q. Have you switched over?

A. We switched over. We only kept it in monitor mode while we demoed it and that was for a good long time. Their recommendation is to keep it in monitor mode for about two or three weeks until you figure out all your variables and get your baseline established. We kept the demo unit in monitor mode for probably a month and a half while we made the decision on our purchase. We ended up purchasing it and we just kept the demo units though we had taken them out of line because our demo had expired. They told us to hang on to them, and then helped us tweak them the rest of the way, get them back on line and gave us a little more training and boom, we were off and running. They actually shipped us a second IPS as a fail over, that was in our purchase agreement and those were put in line for a year. We just upgraded to the new ESM and that upgrade was pretty easy as well.

Q. So no problems there. What problems did you run into?

A. The second IPS we got was dead on arrival. They were really good about replacing it.

Q. What's really good in terms of time?

A. We had a replacement within a week. However, we had been waiting for the ESM for a month and a half since we placed the purchase order. So that was a little frustrating.

Q. You were ready for it and it wasn't ready for you?

A. Right. That was a little frustrating but we got it in. When they shipped it they shipped it with the wrong OS version number on it so we had some implementation problems with that. But we got that worked out. And again, the technical staff was phenomenal and they helped me through that every step of the way. At one point I had four or five technical

people on the phone working with me on it and they just tabled everything else and made sure that we got everything worked out.

Q. You're part of ISSA, which means that you're into the idea of sharing what you've learned, have you found a user group with Nitro that is very helpful or do you just use the SNORT user group for whatever help you need?

A. Mostly I end up turning to SNORT. I've got a number of users of Nitro that I talk to on a routine basis. There are a number of Nitro users in our local ISSA chapter.

Q. Have you worked out access to other users?

A. Yes.

Q. Have you found a consistency in their view? Meaning what you're seeing is what everyone else is seeing or are there sort of significantly different experiences?

A. It seems pretty consistent. The people I've talked to really seem pretty happy. They work with Nitro in one of two ways. They're either more like I am in that they're pretty stable corporate users and they're pretty happy with it or they're more involved in Nitro on the beta test side. I've got a colleague who's at Colby College and he's still beta testing an older release of Nitro but he's about to revamp his whole platform and beta test the latest release of Nitro.

Q. So he's just kind of the leading edge person that companies need to keep their products healthy?

A. Right, but he's really happy with the Nitro products. Nitro worked for him; he pounds it. And that's sort of my experience with the Nitro people I've talked to. They're either really happy or their frustrations aren't with Nitro they're with the fact that there are beta tests and they accept the frustrations that they have because they know they're beta test sites.

"With just a couple of clicks you're at the packet level if you want to be there."

Q. Are they in beta tests because their products very new or because they're upgrading often?

A. They're in beta test because he signed up to be part of the beta test program for Nitro. They just approached me and I've opted not to do it.

Q. It's an appliance, right?

A. It's an appliance and they've got 721D out right now; 723 is slated to come in January or February. They're looking for customers to test it in a real live environment--just like Microsoft does with their products.

Q. How do you know it's really improved security in the organization? Rather than just made you smarter.

A. You set it to just alert and tell you what's going on. You can set it just to patch everything. You can set it up to alert. You can set it up to alert and block or you can set it just to block. You can set it up to alert, block and reset.

I've got it set up just to alert, primarily because we have stuff set up to do it elsewhere. But I can go in and I can look; it's got a huge database and I can go back and look through history and say, how many attacks have you blocked? What have you done over history? I can report on that information.

Q. Do you tell your bosses what it has found?

A. I pull the reports generally about once a month. I give a summary of it and we've got a security brief meeting.

Q. So they expect you to block all the important stuff?

A. Any time I make a change I put it on that change control process which is an automated process and then if it's a major change I go to a meeting and present it as well.

Q. What kind of changes would you make?

A. Well, for example, like I said, just before you called I was making some changes; I was writing some SNORT rules.

Q. And if you change a SNORT rule that's a configuration change that has to be blessed?

**"Technical staff is awesome."**

A. Not necessarily. I just want to keep an eye on it for anything that comes up so I wrote a SNORT filter for it. It just gives me an alert, it's not blocking anything. So it's not one where I'm going to have to go to a meeting, I just put a change control into our system saying informational, here's a SNORT rule out here that's going to give me an alert on this. That way if something goes wrong, it's tracked.

Q. What are the things that have been blocked? Did people say "Oh cool" or has it gotten to be so old hat that nobody notices anymore?

A. Mostly nobody ever notices. I'm pretty much behind the scene so people don't generally notice.

Q. Right, because nothing goes wrong.

A. Right, right. It's got a blacklist feature and a while back Nitro picked up a URL script attack that came across and hit at one of our mobile stations up on one of nursing floors. I went out, verified that it was a bad site that they shouldn't have been to and did a little research and found out we needed to blacklist a slash 16 subnet. We didn't have time to

research everything that we needed to blacklist and make it more distinct so we just blacklisted it. And it brought up a few problems but was that a Nitro problem? No. Was it a poor research and handling on my part? Probably. Were people able to track it quickly? Yeah, because we put it through the change control.

Q. Talk about your environment and where you put this. How many computers are there? How is the place spread out?

A. Right now we have two Nitro boxes sitting on our edge. And they're supposed to be in failover but right now we're passing traffic through both of them. The reason is we have our firewalls on the edge and then it goes from the firewall to the Nitro box and then from the Nitro box to a McAfee spam filter and email virus filter. So we're passing traffic through both channels as opposed to having one in standby and one in primary mode.

Q. Have there been a lot of McAfee issues?

A. No actually it works pretty well. McAfee works pretty well. That's just one we haven't tracked down right now. It's been going on for a long, long time and Nitro found the issue but everything's working fine. No problems at all. We're just passing traffic through both channels.

"My primary criterion was that it give me the information I was looking for quickly and concisely."

Q. How much traffic do you actually have, roughly?

A. We have two T's but one is a load bearing failover and the other is not maxed out.

Q. But you're not running out of the capacity of any of the boxes, right?

A. Oh, no we're nowhere close to the capacity of either of the boxes. We're maybe 10%.

Q. What were your major criteria when you were choosing a tool?

A. Beyond the fact that it be an accurate intrusion prevention system, my primary criteria were that it give me the information I was looking for quickly and concisely. I know that the other folks here wanted it to integrate well into our network, the networking team wanted it to be able to remediate layer three Cisco switches.

Q. And in terms of training to use it, I know you already had a lot of SNORT experience and it's based on that, did they provide anything? Was there anything that you wanted to learn that took a while?

A. Yes. The day of installation they were here for probably half a day because they wanted to spend the day with me just sitting down going through it but it's really very intuitive. And then they spent some time on the phone doing web Training stuff with me. They provide a CD with all their manuals on it for everything and then they're there to answer any questions you have. When we upgraded they spent another day with me just

refreshing stuff. They're not SNORT people though. That's one thing they point out when they show up. The people doing the installs are not, they may be, but they're not necessarily SNORT people. When it comes to writing custom signatures and things like that they've got a nice little utility but it is not necessarily the end all, be all for writing SNORT rules. If you're looking to write custom SNORT signatures generally what they say is write what you're looking for and then send it off to the technical support and their SNORT experts will help you out. And their customer support is the end all to beat all.

Q. In terms of how you use it on a day to day, week to week, month to month basis, what kind of manpower does it require for you and your team?

A. I'm the only one that uses it here other than to troubleshoot specific problems. On a daily basis my usage is from half an hour to about 45 minutes. If I've got a system problem I'm working with or if I'm trying to add in a new device or something like that I may spend a couple of hours.

"It's really very intuitive."

Q. Are there any features that you wish it had?

A. Yes, there are. There are quite a few features and I bring them up to their team on a regular basis. One of the things I wish it would do is give me the ability to drag SNORT rules I'm writing into the appliance I'm

looking for as opposed to writing them in one template and trying to roll them out to another. It doesn't always carry over to the other template so you may have to go in and modify that template by hand.

Q. It's a lot more time consuming then?

A. Right. It's a little frustrating but you know I think that's one of those little quirks that will get fixed eventually. There's an issue with the way you look at your anomaly data, like durations and there's no easy way to tell how long your connection has actually been established. And they're trying to figure out how to fix that. I'd love to be able to resize some of the screens. The way they write their stuff, you can't drag and drop and resize screens like you can with Windows. So your screens are all fixed and that gets a little difficult at times.

Q. How has the response been for the things you've asked for previously? You said you've had it for a year, right?

A. Most of it has been very responsive. The upgrades and features and stuff like that that I've mentioned have shown up in the next release. They come out with releases pretty quickly.

Q. How often do you think the new releases come out?

A. Well, in the year I've had the product they've come out with four releases. They've come out with one major release and three minor releases so it's been pretty good.

Q. How do you feel about NitroSecurity and the ESM you're using overall? Both pros and cons.

A. There are little things I would like to change and little things that are frustrating here and there but you're going to have that with any product you use because they can't do everything for everyone. I've only had it for a little over a year and I had a huge upgrade from the ESS to the ESM. The ESS lets you do just IPSs. The ESM lets you add in SNORT boxes, WMI feeds, firewalls, all sorts of other devices all into your view. That's a huge upgrade for me. It's basically a whole new product for me, so I feel like I'm on a whole new learning curve at this point. There's all sorts of things we can do here I just haven't been able to get people to sit down and look at it because we're 25 people with 2,000 PCs; we're swamped and this is not everyone else's highest priority.

Q. Is there anything you wished we'd asked you that we didn't ask you?

A. If I was talking to people about Nitro I would want them to know is that it's different from the other products I've seen because of its environment. Nitro has an amazing database that allows it to correlate the data and transfer it and look at it faster than anything else I've seen. And the interface on Nitro is absolutely one of a kind and I think if you're going to get in and work with Nitro or work with any intrusion prevention system you're coming in with one of two mindsets. You're either coming with the mindset of wanting a lot of high level reporting and wanting my IPS to basically manage everything. Or coming in with the attitude of getting in and looking at what's happening and doing a lot of the management. And if you come in with the attitude that you want to have your hands dirty and you want to look at what's going on, then Nitro's a good box for you. If you're coming in with the attitude of just wanting a lot of reporting and not wanting your IPS to do a lot of the management, Nitro can still do that for you but the reporting isn't there. Nitro does not do a lot of high level reporting for you. It is not a reporting appliance. It is a here's the data, get your hands dirty and look at it.

SANS Bottom Line on NitroSecurity at St. Joseph's Health Care:

1. Robust IPS with good reporting and trending capabilities;
2. IPS filters unmanageable quantities of data and can be set to alert, to patch or to block and to reset;
3. Database allows it to correlate, transfer and examine data quickly;
4. Can be integrated with SNORT to better view network traffic and allows detailed analysis;
5. Excellent tech support.

**For more information on NitroSecurity:  
Go to: [www.nitrosecurity.com](http://www.nitrosecurity.com)  
E-mail: [salesinfo@nitrosecurity.com](mailto:salesinfo@nitrosecurity.com)  
Phone: 800-795-IPS1**