



WhatWorks in Intrusion Detection and Prevention: Easing the Pains of Compliance at AirTran Airways

WhatWorks is a user-to-user program in which security managers who have implemented effective internet security technologies tell why they deployed it, how it works, how it improves security, what problems they faced and what lessons they learned. Got a story of your own? A product you'd like to know more about? Let us know.
www.sans.org/whatworks

About Michelle Stewart

Michelle Stewart, CISSP, HISP, is the Manager of Data Security for AirTran Airways. She is responsible for Information Security and Compliance. Her day-to-day responsibilities include compliance testing, incident detection and handling and management of security technologies. Michelle has worked in technology for over 15 years, and has an MSMIS with security concentration from Nova Southeastern University.

About AirTran Airways

AirTran Airways, a Fortune 1000 company, offers more than 700 affordable, daily flights to 58 U.S. destinations. With 8,900 friendly Crew Members and America's youngest all-Boeing fleet, AirTran Airways provides XM Satellite Radio and Business Class seating on every flight. For more information and free online booking, visit <http://www.airtran.com>.

SANS Summary

Looking for a solution to ease the pains of PCI compliance, the data security manager for AirTran Airways needed a product that provided increased visibility into network behavior and accountability. It had to be behavior based and capable of collecting information from a widely dispersed network. She found a solution that was scalable, cost-effective and helps to quickly identify and resolve network and security issues.

~~~~~

#### Interview

Q. Tell me about your department. Is it half compliance and half operations or 90% operations and 10% compliance?

A. In my department, security is compliance and monitoring, basically managing risk within IT. Operations is handled by the networking and systems administration teams. We work very closely with Operations to achieve a balance of security and performance.

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

Q. Because there wasn't any reason to act on it?

A. Exactly. So once they started bringing down the hammer--in fact we got fined in 2006--we realized that we should really pay attention. So we wanted to start monitoring some of these behaviors to implement some active controls as opposed to just implementing policies.

Q. Was it for something specific enough that you knew that StealthWatch would actually get rid of or was it kind of general?

A. No, it was a self-imposed ding because at Level II, which is where we are, we fill

out a questionnaire that asks about controls and monitoring activity. We had to say "no" in several instances where we did not exercise controls. So there were probably seven or eight questions on that questionnaire that I had to in all honesty say "no, we don't do that now".

Q. Would you say that the specificity of the PCI and its enforcement has really improved not just compliance at your place, but that you've actually improved security?

A. I would say so. Prior to us prioritizing PCI compliance, we had very limited budget for security monitoring tools.

Q. So it gave you the ability to make sure your systems were secure. What about the systems that don't process credit card data? Are they outside the scope?

A. In some organizations. One of the recommendations to becoming PCI compliant is to limit the scope of PCI. In our environment that doesn't make any sense because we try to take credit cards from wherever possible.

Q. So you're pretty much universal coverage?

A. We want anybody to be able to give us a credit card at any gate or ticket location, any reservation center, any kiosk. We're taking credit cards pretty much anywhere we can touch a customer, on the plane, wherever somebody wants to give us a credit card we're going to take it.

**"We decided to just leapfrog IDS and go straight to Network Behavior Analysis (NBA) because that's where I thought the real problem would be solved."**

Q. So you decided to begin monitoring; where did you go to look for potential solutions?

A. I looked at the security reviews, the magazines, the players out there in the Magic Quadrant and also spoke to colleagues about their experiences. The personal contacts gave me very valuable insight.

Q. How do you describe this category? Is it intrusion detection?

A. I looked at it as intrusion detection, that's correct. Instead of a traditional signature based IDS, we decided to just leapfrog that whole mess and go straight to Network Behavior Analysis (NBA) because that's where I thought the real problem would be solved.

Q. So behavioral analysis is the idea behind StealthWatch. That's its principle strength. Did you decide that you didn't need signatures at all?

A. Well, no we don't because we've got a couple of different tools in concert that made me feel that it was just a waste of time, money and resources. In the past, we did have a signature IDS, but it didn't provide the value we were looking for. We do use signatures in our application firewall because applications are a completely different animal and I felt like we could benefit from an application firewall with signatures but we felt like (another)

signature IDS on the network would overlap too much with behavior analysis and our correlation tool and not provide as much value.

**"Tech support staff is very helpful--and we have always received a response in a timely manner, which sets them apart from other companies."**

Q. Would a log monitoring system have given you that checkmark as well as an NBA?

A. Well, we do have that partially implemented right now and it provides many of our reporting

and correlation requirements. But right now, from my perspective and job function, I get more real-time operational value out of the NBA than I do out of the log analysis. With just a few clicks, I can see exactly who is saturating an interface on the WAN (by network login ID), and what they are doing (i.e http, smb, rdp). I can drill down very quickly to see which systems a particular login ID is currently logged into and where it was used during a certain period of time. Log analysis can get much of the same information, but will provide data only on the systems where we're collecting logs and requires a bit more attention, configuration and training. I think the two solutions really do complement one another, as we feed the NBA syslog to the log analysis system.

Q. What kinds of things does NBA find that other things don't find? What are the kinds of things that it finds that give you a sense that you really have visibility into your networks.

A. The worm detection is quite good. It's worked for us once. Thankfully, I've only needed it once, but that component within the NBA tool helped us out quite a bit. Also, I like the ability to see exactly what behavior is happening at an out-station. StealthWatch can tell

me when a connection is traffic-heavy, but we've got network monitoring tools for monitoring network performance. Prior to StealthWatch, the network folks would have to do some digging to figure out exactly what was going on, and by that time, the behavior may have stopped. Now we can, in a few clicks, see that user 12345 was streaming radio from this time to that time on host XYZ. We allow streaming content for news and other business-related requirements, but we are not supposed to be streaming radio. I can see specifically what's going on and who's doing it--real time--and that's something that StealthWatch is purpose-built to do.

Q. If you were talking to someone else who said, I don't have PCI compliance, but I really, really want to have effective monitoring my security, would you say this kind of tool is really essential?

A. Absolutely.

Q. That the policies are being implemented?

A. I would definitely say that StealthWatch has helped us to enforce policy. I would argue that any organization should have this tool on the short list of requirements.

Q. How do you differentiate between what you can see in a log management tools, log monitoring tools that you can't see in network tools.

A. You can see a lot of specifics. With NetFlow you're not getting any content and within the log monitoring solution, depending on what you're logging, you can get a lot more detail.

"I get more real-time operational value out of the NBA than I do out of the log analysis. I can drill down very quickly."

Q. But you can go back and find out who did what essentially with log monitoring?

A. Yes.

Q. The forensics is much better on the log monitoring?

A. That's absolutely right. I think they do integrate well because you get the details in the log solution. You might see something of interest on StealthWatch, like a big file transfer between an internal system and an external system that doesn't seem appropriate. Then you can go to a log solution and determine the particulars of the transfer.

Q. So you could even say NBA is more of an early warning system or a higher view of what's going on in your network?

A. Yes.

Q. You were looking at IDS and somehow you made a decision to go with the behavioral based instead of the signature based which almost everybody else does, right? Did you have to talk people into that or was it just your decision and you said let's do it.

A. No. Actually it was well received by our senior management because prior to hiring me, they attempted to implement IDS and there were just too many false positives. It was completely useless from their perspective and it has since been decommissioned. So they were completely turned off on signature based anyway.

Q. So it had run its course and proposing that would have just been silly?

A. Yes, it was unacceptable and it wasn't even something I was looking for anyway. I thought behavior was going to give us better information than signature-based with a lot fewer false positives. After a tuning exercise that was exactly the case--we don't get a lot of false positives.

Q. Were there 10 choices, two choices, only one choice? How many different tools did you look at once you decided to use a behavior based tool?

A. Well actually it was only one choice based on the constraints that I had to test in my environment. My network director said: "you can't touch this, you can't do that and I won't change my network flow to going over to your appliance". With those constraints, Lancop came over with a flow replicator appliance that was able to sniff the NetFlow traffic from a core switch. So instead of the network traffic being pushed to the NBA appliance, the

"The worm detection is quite good."

collector, we were able to sniff the traffic that was actually intended for existing network monitoring tools. With it in place we were able to test the solution within our environment. Lancop provided the proof of concept and the testing and

they had an engineer here to set it all up. It worked very well for us.

Q. And the network guys didn't fight you?

A. Initially they did. We decided to put it in as kind of an overlay rather than as an in line tool. We're still sniffing traffic, but I want to change the config on all of our network devices to send NetFlow data directly to StealthWatch. The task has not been a priority for our network team.

Q. And when it went live did it still work that way as an overlay? Or after it proved itself did you change the architecture to fit more?

A. The intention is always to change it to have the NetFlow data being pushed through the appliance but it is still in as an overlay. It was really very low impact from a concept perspective and we had absolutely nothing to lose. So they put it in, it sniffed the traffic and it did exactly what it said it was going to do and we've been extremely happy with the results. It's been over a year now and I've had the intention of changing our configuration on the network devices to push the NetFlow data to our network directly because I do see

some black spots. We're not getting 100% of the traffic. I'd like to change that model but it has given us the flexibility of operating for a year and getting 95% of all the information I need just by sniffing.

Q. Of all the things it found early, which are the ones that made you feel best about it? The worm?

A. Well, in that particular case, I got the alert for it and started looking into it; it identified a particular system as a propagator. StealthWatch identified all of the systems that it "touched", communicating a manner that is consistent with worm behavior. By looking at the worm detection analysis tool I was able to pinpoint specific workstations, shut down those key systems and very quickly contain the issue. We were able to contain the situation quickly and that did make me feel good about having the product in place. Additionally, there have been cases in very limited forensics where somebody wanted details about network behavior. For example, if a user states: "hey, somebody remoted in my machine and didn't identify themselves", I am able to go to that machine and see a remote stream from PC A to PC B. PC A had user 12345 logged into it at the exact same time that the remote session was open so this person is responsible for that behavior.

Q. You got that without the log?

A. I got that from the flow data, that's correct. The appliance can keep up to 14 days of detailed flow data so if you need to do some limited forensics over that timeframe it will tell you who did what when. But it's also the beauty of NetFlow because it's very low overhead; it's very efficient.

Q. You had talked about worm detection, is that the best way that you know it improved security for you or are there other ways too?

A. No there are definitely other ways. We have a very distributed environment, a lot of wide area network locations. Prior to this tool, the network engineers had to do some digging to figure out what was going on. Now all we really have to do is click a couple of buttons and determine that Pittsburgh is saturated because they're doing their e-learning; they're streaming video--appropriate behavior. It's appropriate business use, but if someone is experiencing network latency issues, then we can tell the person to stop doing the video. So it's really helped us in some operational areas where we wouldn't be able to see that very quickly or easily.

**"I'm very happy with the product. I think it's solid and it does exactly what I need for it to do."**

The security concerns that I have are also around who does what when. StealthWatch is not only useful in satisfying Requirement 11 of PCI, but also Requirement 10. I think that the remote session example is a very good example because prior to this tool we would know that anybody in a particular IT group could have remote access to this laptop, but we would not have a way to tell exactly who opened the session. We didn't have any real audit trail

for any of that stuff, and no one would feel compelled to own up to the behavior. I think it's very important for compliance and security because now that it's being audited, people are more inclined to follow that straight and narrow, especially when they're logged in under their own ID.

Q. Beyond wanting a network behavioral analysis tool, what other kinds of criteria did you have?

A. The audit trail was a big one: the accountability aspect, because prior to this we didn't have that. It's not a requirement for the Lancope NBA product, but an add-on identity correlation appliance that is optional in the StealthWatch suite. Sure, it's good to know that "somebody's" streaming radio or that "somebody's" doing a remote session, or "somebody's" trying to use PC Anywhere, but who's doing it is more important so you can take some action.

Q. How was it to install?

A. Actually very easy. In one day the engineer came in, put the appliances in and we started sniffing the traffic. We didn't change any of our environment to accommodate it, we just sniffed. We did have one difficulty and that was that we were at a higher version of NetFlow than they supported on that appliance, so they had to upgrade, which they did fairly quickly. Then we started seeing the NetFlow traffic. So the initial implementation was unsuccessful because of the version of NetFlow that we were using.

"The management console is just incredible. The analytical capabilities are awesome."

(StealthWatch now supports all versions of NetFlow.)

Q. Did that require tech support?

A. Their implementation engineers were the ones that handled all that.

Q. Have you had any need for tech support since then?

A. Yes, I have. We have had a couple of instances where it stopped seeing certain traffic or it's locked up and their tech support has been very responsive in getting us right back on track. Very little downtime.

Q. In terms of training to use the tool in the way that you use it, did it require someone to come out, did they do WebX? How did you learn?

A. They did have someone come out and I'm sure that that's made it a whole lot easier because they are local. The engineers and phone support staff are very helpful--and we have always received a response in a timely manner, which sets them apart from other companies.

Q. And what about manpower for it?

A. It doesn't really require a lot of maintenance. Three of us in security actually look at it on a daily basis. We have the console up all the time on one of our screens. But maintaining it or doing updates requires very little hands-on effort. We do something maybe once a month if even that. Once we did the initial implementation and the tuning and setting up the zones, which took probably 80 man hours to set it up, tuning it, tweaking it, and then once that exercise was completed then it's just running.

Q. How did you get the money to justify the NBA?

A. I didn't need to make the case for this specific tool. What I did make the case for was the need to spend money to become PCI compliant. Senior management supported that and as a part of that presentation I had several projects, implementations that I had mapped to PCI requirements, and NBA was one of those.

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

A. While its analytical capabilities are supreme, it only recently added the ability to customize and schedule compliance reports. I just received WebEx training on that new feature. Some of our other tools have compliance-specific reporting content bundled with the products. I think that would be useful in this case.

Q. But that's not anything you've asked them for yet?

A. No, it isn't. I've just really been too busy. I think their management console is just incredible. I love the way that you can just slice and dice information and right click and get different flow reports from endpoint to endpoint. The analytical capabilities are awesome. I'm an analyst at heart and I just love the ability to dig deep, any way you want and they do a real good job with that. I'm pretty happy with the management console.

**"I would definitely say that StealthWatch has helped us to enforce policy. I would argue that any organization should have this tool on the short list of requirements."**

Q. How you feel about it overall?

A. I'm very happy with the product. I think it's solid and it does exactly what I need for it to do. We've only had very few instances where it's locked up or we've had to restart. From a performance perspective it works great. It handles the traffic that we throw at it. I think that I get a lot of benefit out of the product. I like it a lot.

Q. How does StealthWatch interact with NetFlow from Cisco? You talked about the fact that it can overlay so it doesn't have to actually change the architecture, but its principle data source is NetFlow data right? Or does it take other data as well?

A. The collector and the analytical piece take NetFlow data, but I'm not aware of its additional capabilities.

Q. It doesn't look at firewall logs or anything else?

A. No. It just looks at the NetFlow data. As far as I know, it doesn't look at firewall logs.

Q. Were you were able to find remote access, people trying to use their machines from home?

A. Yes. That is obviously against policy and we just educated those users a little bit better. It helps us to target our education. It's not people trying to do bad stuff, just trying to get more work done in a day. We can identify the policy breach and try to resolve the business need another way. If someone were trying to do something maliciously, this type of tool could detect them.

Q. How does it help you determine risk reduction?

A. I've got my zones set up to isolate nodes by function or risk and then I dictate an appropriate behavior policy on each zone. If someone's trying to remote into one of these PCs and they're not supposed to be, I'll know about it. If activity that is inappropriate for the zone starts to occur, then StealthWatch throws a policy violation. It helps me to determine and identify risk on a host level even.

SANS Bottom Line on StealthWatch at AirTran Airways:

1. Provides good visibility into network behavior, including remote access attempts;
2. Automation aids log analysis for a widely dispersed network;
3. Simple implementation and low manpower requirements make it cost-effective;
4. Aids in PCI compliance.

**For more information on Lancope**  
**Visit: [www.lancope.com](http://www.lancope.com)**  
**E-mail: [sales@lancope.com](mailto:sales@lancope.com)**  
**Phone: 888-419-1462**