

**Intrusion
Prevention
Tools for
Defense
In-Depth**

**SANS WhatWorks
in Internet Security**

**TippingPoint
at
Sara Lee**

2006

TippingPoint at Sara Lee



About Sara Lee

Sara Lee Corp. is a global manufacturer and marketer of apparel, food and food service products for consumers throughout the world. It has operations in 58 countries and markets branded products in nearly 200 nations. Sara Lee Corp. employs 137,000 people worldwide.

About Bryan Jordan

Bryan Jordan and his group: architect and manage Sara Lee network operations and its network security appliances. He has worked there for three years and is responsible for network and network security architecture, as well as security administration.

SANS Summary

Nasty virus outbreaks at Sara Lee motivated the company to try an intrusion detection system. The company tried Snort, but found it too labor intensive for such a widespread and diverse network, prompting it to seek a simple to use commercial IPS.

~~~~~

To hear Bryan Jordan expand on the answers below, 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>.

~~~~~

Interview

Q. What was happening at Sara Lee that led you to look for an intrusion prevention system?

A. The network environment had a few, limited, virus and worm outbreaks

"We had trouble finding the magic bullet... TippingPoint best met our needs. A week later we felt our tests were validated by TippingPoint winning the NSS Gold award."

that cost parts of the business a number of hours of downtime. We had little in place and business demands instantly changed our perspective.

Licensing with some of the commercial products was a real turnoff and we wanted something that would be transparent.

Q. How did you approach finding a new solution?

A. It was a very lengthy process. We had not evaluated products of this type previously. We knew what we wanted but had trouble finding the magic bullet. We looked at several (network/security) vendors in addition to TippingPoint. We eventually had a bake off and TippingPoint best met our needs. A week later we felt our tests were validated by TippingPoint winning the NSS Gold award.

Q. What product did you finally select and why?

A. We selected TippingPoint, but it was not the only solution. We implemented a multi-vendor IPS environment.

Q. What were the criteria you decided were most important?

A. Our main criteria were what product(s) provide the least intrusive end user experience and actually worked.

Q. What was the deployment process like?

A. They sent an engineer and we put the box in. We kept it in monitor mode for a week and then turned on block mode. It blocked some stuff we used for commerce, but otherwise, bad traffic was labeled bad and good was good. We checked it a few times a day and the logs reflected the traffic we were seeing.

Q. Where on the network is the appropriate place to test block mode?

A. Any place we needed to protect Sara Lee intellectual property and network resources.

Q. What problems arose?

A. One day we tried to go beyond the recommended settings and blocked instant messaging and some cookie based reporting applications. It turned out we used a similar application to track sales on one our business-to-business Web sites. Once the help desk call came in it was easy to identify the problem and the resolution needed.

"We deployed the IPS any place we needed to protect Sara Lee intellectual property: HQ, data Centers, campuses."

Q. How difficult was that?

A. It was harder to find the source destination or service then it was to fix. It took about five minutes. We use pretty much the entire RFC 1918 private IP addressing range and have a number wan circuits that are DS3 and above. It was harder to find and understand where the source IP was in the network than to actually change the rule to allow the traffic.

Q. Where did you deploy the IPS?

A. Any place we needed to protect Sara Lee intellectual property: HQ, data Centers, campuses.

Q. What level of senior management approval did you get?

"Technical support was very good; I have called at all times of the night and gotten knowledgeable people."

A. Once we showed upper management the potentially bad traffic within our network it was an easy sell. This was especially true after we demonstrated the number of users accessing external resources against policy.

Q. Were there any internal problems that you found because of TippingPoint?

A. Bandwidth issues were previously misdiagnosed. The download of media files was much more widespread than previously thought. It also showed that some of our applications were using random ports rather than adhering to IETF standards.

Q. Did you have any technical issues?

A. A big painpoint was a "feature" that would set the ports back to factory settings because it didn't like to work with Cisco. After I complained, that "feature" went away in the next release.

Q. How was technical support?

A. It was very good, especially knowing how small they were before the 3Com acquisition. I have called at all times of the night and gotten knowledgeable people.

Q. Was there an impact on network load?

A. It is a concern, but we sized ours appropriately.

Q. What level of manpower does it require and how much training did your staff need?

A. I spend about two hours a week doing signature and software updates.

"We began with four of their systems and have grown a bunch more. Having it has been great for the network."

Q. Are there any features you would like to see added?

A. Since we like to keep IPS in each network geography as close to the edge as possible, I would like to see a feature to decrypt encrypted tunnels, IPSEC or GRE so that we can monitor all traffic incoming and outgoing without having to pass through a number of devices to be sure of packet inspection.

Q. How do you feel about TippingPoint over all?

A. We began with four of their systems and have grown a bunch more. Having it has been great for the network.

~~~~~

**SANS Bottom Line on TippingPoint at Sara Lee**

- 1. Simple deployment and use.
- 2. Limited manpower needed for monitoring and support.
- 3. Few false positives.
- 4. Responsive customer service.

**For more information on TippingPoint:**

**Visit: [www.tippingpoint.com](http://www.tippingpoint.com)**

**E-mail: [info@tippingpoint.com](mailto:info@tippingpoint.com)**

**Phone: 888-TRUE-IPS**