

## *What Works in Intrusion Prevention*

About T. Rowe Price Investment

T. Rowe Price, headquartered in Baltimore, Maryland, is an investment management firm offering individuals and institutions around the world investment management guidance and expertise.



About Scott Davis

Scott Davis manages the network security group within Enterprise Security at T. Rowe Price. His group is responsible for security infrastructure including firewalls, intrusion prevention, proxies, vulnerability management, and the anti-virus, anti-spam infrastructure, as well as incident response. Before getting into the security field, Scott worked for Marriott where he was responsible for that company's web farm of servers and Intranet.

SANS Summary

T. Rowe Price has approximately 1,000 servers and users all over the world -- London, Tokyo, Hong Kong, among other places. Senior management, auditors and network security staff needed a reliable IPS system to protect their applications. The intrusion prevention product they bought ensured compliance with Sarbanes-Oxley, led to a radical decrease in spyware by more than 80%, was easy to deploy and to maintain, and protected the company's servers from exploits that would have made it through their firewall without it.

~~~~~

*Interview*

Q. What led you to look for an intrusion prevention system?\*

A. The key driver was regulatory compliance. Senior management was reviewing plans for Sarbanes-Oxley compliance, and the audit firms that were helping in planning suggested that companies would fare better in the SOX audit if they had intrusion prevention systems in place.

At the same time we in network security recognized that we needed a way to fully protect our applications against application exploits. We knew of no other way to block spyware and application exploits.

*\* To hear Scott Davis expand on the 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>.*

**“When we put in our IPS, the spyware connections dropped from more than 130,000 to fewer than 20,000.”**

Q. You mentioned spyware. Is that a problem that you see IPS helping to solve?

A. Yes. Spyware was being delivered via browser exploits. Once we had the IPS in place, we found spyware on client computers was trying to connect to information collection

points outside our organization. When we put in our IPS, the number of spyware connections dropped from more than 130,000 to fewer than 20,000. The IPS simply blocked the connection from the spyware on the client computer trying to phone home.

Q. Why does some still get through?

A. First of all no vendor can keep up with the number of infections out there. The hits we see now are the attempts to download the initial spyware application. In addition we have people taking laptops out of the organization, the laptops get infected on public or home networks and then come back in. In some cases, stationary desktops get hit before the IPS filter comes to us.

Q. Thanks for that clarification of spyware and IPS. Let's go back to the IPS evaluation process. When did you begin it and what steps did you take?

A. We started the evaluation last year (2004) in July. We reviewed Gartner and Meta reports and security trade publications, performed Google searches and contacted vendors to find out who the big players were. That process narrowed our search down to three possibilities, all of which, it turned out, were in Gartner's first quadrant.

Q. Which ones were they? And can you tell us about the evaluation process?

A. ISS Proventia, TippingPoint, and Juniper Networks IDP. We brought all two of the three IPS boxes into the lab and we simulated traffic: first legitimate to see if it stopped traffic that should not be stopped; then attack traffic to see if it caught malicious traffic.

They all did well on those tests.

Q. Were there any other criteria that mattered?

A. We needed the system to handle at least five gigabits throughput. Both TippingPoint and Juniper could do that.

Then we started evaluating the deployability and usability. These were very important to us because we have a small staff. We need the tools to be easy to deploy and to maintain without a lot of care and feeding. We wanted the tools to show results fast.

Q. How did they do on those tests?

A. One of the products made the deployment problem very cumbersome. We had to wade through thousands of filters (and we had a diversified environment) determining which ones needed to be enabled. The other one, TippingPoint, shipped with recommended settings, an out-of-the box configuration with a set of filters set to block by default and those settings just worked. All we had to do extra with TippingPoint was turn on a few for specific applications. The product came in, we plugged it into our environment, accepted default policy, and it started working immediately.

Q. Sounds like TippingPoint won the throughput and ease of deployment battle. How did it do on price?

A. TippingPoint was a little higher than Juniper; but we would have had to hire more security analysts to manage Juniper so the extra cost of TippingPoint was justified.

Q. How did you do the roll-out?

A. We were already testing the system. As we got closer to the roll-out, we ran production traffic in sniff mode (without blocking). We set that up outside our public facing firewall for ten days to see whether it dropped legitimate traffic. Other than monitoring issues with ICMP, there were no problems at all. That gave the network team a great deal of confidence in the system.

**“This product came in, we plugged it into our environment, accepted default policy, and it started working.”**

Q. I want to ask about the number of intrusion prevention systems you deployed, but first can you tell us about your environment -- numbers and types of systems?

A. We have 5,000 desktops and about 1,000 servers. Most are located in two buildings in Baltimore and Owings Mills. Users are all over the world: London, Tokyo, Hong Kong, plus many others.

Q. How many TippingPoint IPS systems did you employ and where did you put them?

A. In 2004, in our initial deployment, we installed four boxes. One went on the public facing Internet connection (watching traffic going in and out); another was installed to

protect our remote access, VPN, Dial-up and ISDN connections. We also used two for our third party connections to Bloomberg and other financial reporting partners (one for each of the two buildings).

Now in 2005, we are installing more for domestic high availability so we can have failover.

We used different size boxes for different connections -- just matching bandwidth use to capacity of the TippingPoint devices.

Q. How long did it take and how many people were required to get it operational?

A. One security engineer was responsible, and it took us a month. It was that long because we do infrastructure changes between 3 and 5 AM on Sunday. We decided to put the boxes in one per week.

Once the boxes were in, we put them in sniff mode for a week, to make sure no critical system would go down.

We put another 15 in, mainly to protect remote offices, during 2005. It required half of a full-time employee to do everything from ordering, bringing in, configuring, shipping to the remote and international offices and coordination with offices. The hard part was finding people in each remote office to rack the devices.

**“In initial deployment, we installed four boxes. Now we are installing more for domestic high availability so we can have failover.”**

Q. Did you find any problems that needed fixing during deployment?

A. There were some tweaks necessary: HP Openview and homegrown scripts that our network folks use to monitor boxes rely on ICMP. It is all legitimate traffic but it triggered an ICMP anomaly alert in TippingPoint. So we set up the

system to accept that traffic only from specific IP addresses.

Q. What did it take to get management approval for the purchase?

A. We did a lot of cost justification. Our main theme was that if we could deploy this, not only could we be compliant with regulations, but we would also improve security. As a bonus, the business users would not be down for days while we replaced their machines that might have become infected if we didn't have the IPS. If a worm gets loose, and 50% of the IT staff has to clean up, many of the business users are out of business.

Most of the justification was at IT management (CIO/CTO) and finance level.

Q. What types of questions did they ask?

A. There was a series of questions: what is it, what is it capable of, whom will it impact, what is the product environment, what kind of high availability. It was new and, especially for the network folks, it was scary.

One of the best things we did in explaining it was to use the firewall as the model. We showed them that traffic that was allowed through the firewall can still have exploits.

Q. The bottom line question. How can you prove that the IPS actually improved security for T. Rowe Price?

A. One that we have already talked about is the radical decrease in spyware by more than 80%, but that was a side benefit. Our main goal is to stop application exploits. In the past we would have heard about a vulnerability, and we would have researched it to figure out what applications would be impacted, and then manually blocked ports. We were never able to stay ahead. Now all that research and blocking are done centrally by TippingPoint, and the filters are in place far earlier than we could have ever produced and tested them.

**“Now all that research and blocking are done centrally – and filters are in place far earlier than we ever could have produced and tested them.”**

The way we know the filters actually improve security is that we have an IPS protecting our customer facing web applications. We see Slammer, port 445 and SQL Server exploits, and exploits that normally come through on port 80. Some of these exploits would have made it through the firewall and infected the production systems. Because of our IPS deployment, the servers were never touched.

The most recent example was the Windows Plug and Play- vulnerability that recently resulted in the Zotob worm- within an hour or two of the vulnerability being announced, we had a filter in place. This was prior to the existence of the Zotob exploit. Two days after the vulnerability was announced, exploit code was published. At other organizations I am familiar with, more than half the staff was still running Windows 2000. Their machines were compromised by the Zotob worm and down for more than 24 hours. Our Windows 2000 environment was protected until we could deploy the patches from Microsoft.

**“From the very beginning, the tech support people have shown an ‘I am here to help you’ attitude’.”**

Q. How have you found TippingPoint’s technical support?

A. From the very beginning, the tech support people have shown an “I am here to help you” attitude. And we have had the same experience all through the process. We had to call them when we saw some newer filters acting

strangely, causing the box to alarm (not blocking traffic) on anomaly detection. When that happened, TippingPoint modified the filter or gave us an interim patch. They do at least one deployment a week and we have had only three of four of these issues in all the time we have had the system.

Tech support is live (not an answering machine). There is local support team of a system engineer and a sales person out of Atlanta who covers the east coast, and they are the best I have ever seen from any vendor. They even come by frequently just to make sure everything is working well.

Q. Does the IPS slow things down? In other words, what network latency have you experienced?

A. We have not seen any slowdown at all. When we deployed the TippingPoint solution we sized the boxes to exceed the network throughput at our current levels. This would leave us room to grow network bandwidth in the future.

Q. Would you recommend it to other organizations?

A. I already have. I have provided feedback for potential TippingPoint customers and to peers within the financial services industry.

**Q. “Would you recommend it to other organizations?”  
A. “I already have.”**

Q. Since you originally deployed this for compliance purposes, do you feel intrusion prevention has been a valid and effective technology for you?

A. Yes it has. We have been able to show both internal and external auditors evidence of attacks blocked, a reduction in Spyware infections and tracking of asset protection.

*(continued)*

SANS Bottom Line on TippingPoint at T. Rowe Price

1. Number of spyware connections dropped by more than 80%
2. Tools are easy to deploy and easy to maintain
3. System shipped with recommended settings that just worked
4. Tech support is live (not an answering machine) and the local support team is excellent.

For more information on TippingPoint  
visit [info@tippingpoint.com](mailto:info@tippingpoint.com)  
or call  
(888) TRUE IPS (888-878-3477)