



Leading Logistics Provider, Transplace, Improves Network Security and Availability with TippingPoint IPS

The Challenge

Transplace is a non-asset based third-party logistics (3PL) provider offering manufacturers and retailers logistics technology and transportation management services. Its logistics technology is used to design, optimize, and manage complex supply chains, serving its customer base of 500 manufacturers, retailers and food & beverage companies. As one of the top ten freight capacity brokers in the U.S. and a leading provider of 3PL services, Transplace generates revenue in excess of \$700 million from approximately 650 customers.

Its core technology is the Transportation Management System (TMS), a fully integrated web-based transportation platform that customers use to collaborate on transportation logistics strategy, planning and execution. Since it is delivered via software as a service model, it is critical that the system be up and running all the time.

“We have 15,000 users accessing the TMS at any given time and since our main users are working at all hours, the system must be available 24 hours a day, seven days a week,” said Scott Engel, Director of IT Infrastructure at Transplace. “Ensuring service continuity is our number one priority. If a system slows down, or worse is taken offline, it can affect millions of dollars worth of shipments. We needed visibility into the vulnerable areas of our network, allowing us to continuously

keep it protected from the bots and phishing attacks that consume bandwidth and threaten downtime.”

Solving the IPS Problem

One of the first challenges Transplace needed to address was securing the FTP site for its customers. The Transplace TMS relies heavily on FTP so customers and partners can post information and communicate with one another quickly. However, since this requires the FTP port to be relatively open, the company was seeing a tremendous amount of brute force attempts on this segment. “We knew we needed an intrusion prevention system (IPS) to help us quarantine the IP addresses that were attempting to access our FTP site,” said Engel.

“We evaluated solutions from a number of vendors offering IPS solutions, but TippingPoint was the only one offering the quarantine option that would help us address the brute force attacks on our FTP port,” said Engel. “We also really liked the overall support structure and the Digital Vaccine filter service that updates the IPS filters every week.”

In 2006, Transplace deployed several TippingPoint IPS units at their headquarters in Dallas, as well as their data center in Lowell. In addition, the company purchased a Security Management System (SMS) to provide easier deployment and management of the filters in the IPS.

“The SMS allows us to see the types of attacks that are hitting us. We can also use it to set and enforce policies for things like instant messaging and P2P application usage.”

Scott Engel,
Director of IT Infrastructure,
Transplace

“The SMS allows us to see the types of attacks that are hitting us. We can also use it to set and enforce policies for things like instant messaging and P2P application usage.” said Engel.

Following a successful deployment of the TippingPoint IPS, Transplace was looking for guidance on tuning the filter settings to be more effective. Additionally, they wanted a way to quickly view the status of the IPS filters relative to any new vulnerabilities found in their network.

Improving_the_value_of_IPS_with_Vulnerability_Management_from_Critical_Watch

In 2008, Engel and his team started looking around for a vulnerability management (VM) solution that would help them to easily identify weak points on the network. “As part of our research we had heard that TippingPoint was working with vulnerability management vendor, Critical Watch, to integrate VM with the IPS. We found that to be an extremely valuable addition to the IPS capabilities,” said Engel.

The Critical Watch FusionVM product queries the TippingPoint SMS to provide Transplace with a comprehensive view of the vulnerabilities on its network, correlated with the related Digital Vaccine filters in the TippingPoint IPS. The resulting reports include information about the status of individual Digital Vaccine filters – including whether they are activated or off; set to block, permit or notify; or configured for quarantine or rate limiting.

“TippingPoint identifies the vulnerabilities and filters, but if you don’t know the current state of your network environment, you don’t know what patch or how you should be utilizing the filters,” said Engel. “The integrated VM/IPS solution not only gives us a view of our entire system and where we are vulnerable, it also identifies what TippingPoint filters are available to us and the current status of those filters. We can instantly see where our network needs protection and quickly make the changes that enable this protection.”

The_Results

For Engel, TippingPoint provides very powerful security protection for vulnerabilities – particularly ones that have yet to be patched by the vendor.

“Vendor vulnerabilities are reported all the time, but it can take several days or even months before they can issue patches for these. We can’t take the risk that an exploit will take advantage of one of these vulnerabilities and take our system down. The TippingPoint IPS provides the protection on these vulnerabilities during that gap of time between when the vulnerability is announced and a patch is available,” he said.

Further, TippingPoint saves Transplace several hours a week just by eliminating the need to manually block the IP addresses that are attacking the FTP port. They can also easily identify machines that potentially have spyware loaded on them before users have performance issues.

Finally, the IPS with integrated vulnerability management provides even more value in terms of time savings. “It really speeds up the process of determining where we are vulnerable and what we can do about it – or better yet, show how the vulnerability is already being addressed. If I had to go through the filters manually it would take several days to identify and match them up with the individual hosts and vulnerabilities and now I can see that from a single screen.” said Engel. “I can definitely say this makes our network much more secure and it gives us confidence to know we have the correct filters deployed for our environment.”

Corporate_Headquarters: 7501B North Capital of Texas Hwy. > Austin, Texas 78731 USA > +1 512 681 8000 > +1 888 TRUE IPS
European_Headquarters: Herengracht 466, 2nd Floor > 1017 CA Amsterdam, The Netherlands > +31 20 521 0450
Asia_Pacific_Headquarters: 47 Scotts Road #11-03 Goldbell Towers > Singapore 228233 > +65 6213 5999

