

Corero IPS Does Everything for Pep Boys: Protection, Reliability, Flexibility

Summary

Industry: Automotive parts and service

Challenge: Protect Pep Boys' network of more than 700 stores and corporate headquarters against malicious attack that could result in the theft of sensitive customer and employee information.

Solution: Corero's IPS

Results: The system cost-effectively protects Pep Boys' networks against attack, providing high reliability, excellent support, flexibility for environment-specific controls and timely updates against the latest threats.

Key Benefits

- Stops advanced threats out of the box
- Outstanding performance; lowest latency, superior throughput
- Reliable, purpose-built hardware
- Fast, easy deployment
- Blocks, malware, spyware, viruses and botnets
- Compatible with distributed networking architecture

From a modest beginning in 1921, when four Navy buddies -- Emanuel "Manny" Rosenfeld, Maurice "Moe" Strauss, Graham "Jack" Jackson and Moe Radavitz pooled together \$800 to open an auto supply parts store in Philadelphia, Pep Boys has grown into a multi-billion dollar automotive services and retail chain, with more than 700 stores across the U.S. and Puerto Rico. The familiar caricature logo featuring three of the founders' faces, and catchy motto, "Pep Boys Does Everything for Less," are part of American business culture.

The Challenge

Behind the three faces on the ubiquitous Pep Boys logo is a major, successful nationwide corporation, whose business and customers must be protected against increasingly sophisticated cyber-attacks. Pep Boys is the custodian of myriad customer and employee records from well over 700 stores, as well as its Philadelphia corporate headquarters. Personally identifiable information (PII) and corporate data are valuable targets for cyber-criminals. As an e-commerce company, Pep Boys is entrusted with a large amount of customer information and employee data, such as Social Security numbers, especially given the high turnover in its stores due to young workers holding short-term and seasonal jobs. Pep Boys also stores customer information through its online "Glovebox" feature, which enables customers to record and conveniently access information about their vehicles and service history.

Firewalls are essential to control access to Pep Boys' corporate network and the sensitive data it holds, but far from sufficient in today's threat environment.

"Firewalls are just firewalls," says Pete Bottcher, Pep Boys Information Security Officer. "They block ports, block IP addresses."

Meanwhile, on the dark side, organized criminals have access to the most sophisticated attack tools and have at their disposal huge armies of compromised computers -- often tens of thousands -- organized into botnets that can be rented for \$100 or less. Attacks are more sophisticated than ever, making use of obfuscation, polymorphic techniques and sheer volume -- millions of unique malware samples identified each year. Targeted attacks, sometimes exploiting previously unknown or zero-day vulnerabilities are a frequent concern, particularly for high-profile companies. Criminal attackers have the upper hand over most traditional defenses, such as desktop anti-malware, which is essential but inadequate in the face of this onslaught.

"Organized crime is hiring the best people," observes Bottcher. "They're getting paid better and working for the other side."

Compliance is also a concern, as Pep Boys is subject to PCI DSS. While the automotive giant does not store credit card information, which is encrypted at point of sale (POS) devices and outsourced for processing and storage, Bottcher says compromised POS devices are a risk. And, as a nationwide business, Pep Boys is subject to the more than 40 state data breach notification laws, which generally require notification of customers in the event of suspected information breaches. Bottcher pays particular attention to emerging state data protection laws, which are quite demanding, led by Massachusetts 201 CMR 17.00 for protection of personal information.

The Solution

All of this information flows back and forth between the Philadelphia offices and Pep Boys' stores: All the stores access the Internet through single point of entry at corporate headquarters, which becomes the critical control point for protection against Internet-borne threats. Pep Boys deployed intrusion prevention systems to protect its corporate networks and, by extension, its store locations, but ran into issues when it came time to replace its older TippingPoint product with new technology.

The result was that Bottcher elected to replace TippingPoint with Corero Network Security's IPS, a decision with which he's been very satisfied. He had a service issue with TippingPoint, which caused him to question whether he should continue with that vendor.

"The sales people disappeared. I couldn't get anyone to call me back," he recalls. The experience left Bottcher with concerns over vendor support.

"What about management of the IPS?" he says. "How can I be guaranteed I will get my security updates on time if they are not handling everything else correctly?"

Frustrated by his efforts to replace his TippingPoint IPS, Bottcher began looking for alternatives. He attended a Corero seminar and liked what he saw. The Corero solution was deployed at Pep Boys for a proof of concept evaluation based on policies and rule sets customized for their environment. He liked the flexibility he had to run the IPS – or a specific rule being tested – in bypass mode so he could observe the potential impact on both unwanted and legitimate traffic without consequence during testing.

Bottcher found the dashboard easy to monitor in his office and was pleased with the results – and the price – and committed to Corero.

He was impressed that Corero's IPS is built on the flexible and powerful 64-core Tiller processor-based hardware platform. "It was brand new, and I knew it would be good for years to come." He knew that Corero's IPS would be highly reliable (20 to 30 year mean time between failures) because of its architecture.

"IPSeS should not need routine maintenance. It's not something I should have to worry about," he declares. "If you have an engine and an electronic motor, which will last longer? The electronic motor, because it has fewer moving parts."

Bottcher was also impressed with Corero's ProtectionCluster capability, which allows his two IPS appliances to perform load balancing for performance and, at the same time, provide high availability in the unlikely event of failure.

"Corero installed the IPS, and I really don't have to worry about it."

The Results

Corero's IPS has kept Pep Boys' network and the information that is critical to its business protected 24x7. Bottcher, who is responsible for the company's security, monitors the IPS from

his office, where he can investigate suspicious traffic – "anything abnormally high that sticks out, such as unusual DNS traffic or UDP probes" – and view alerts through the intuitive dashboard. The network visibility not only affords security but has enabled Bottcher to solve some network operational issues and improve performance in the bargain.

Monitoring outbound as well as inbound traffic is useful as well. Monitoring outbound traffic can help identify infected computers that are communicating with their command-and-control servers or being used as part of a botnet attack. It can also be used to monitor traffic which may not be malicious but may reveal the use of unauthorized applications.

"We're pretty tight inside, but it helps to see if traffic is repeatedly going to an IP address it should be going to," he says.

The log-based reporting features enabled through the Corero Network Security Analyzer (NSA) security information and event management (SIEM) tool is particularly useful during PCI DSS audits, he adds.

Bottcher gets timely updates to protect Pep Boys and its customers against the latest threats, and likes the information and recommendations that accompany them. He uses this information to apply updates based on Pep Boys particular environment. For example, one update came with an advisory for Lotus Notes users (such as Pep Boys) because of possible issues, recommending the rule be set in bypass mode or tested before rolling it out. "But for high-profile updates, they recommend blocking -- and we block."

Bottcher also likes the rollback feature, which allows him to revert to previous software versions if there is an issue.

"And the support is fantastic," he says. "I call or open a ticket online, and within 15-20 minutes someone is calling, depending on severity. Even with low-severity cases, I get an email, letting me know Corero is working on the issue and asking if there is a convenient time to call."

Above all, Bottcher values Corero's IPS for its reliability and flexibility.

"Corero gives me both," he says. "It has the flexibility to run in bypass mode to test and troubleshoot: Every company has its own idiosyncrasies, such as legacy software it is still relying on. And it has the reliability in terms of being a reliable appliance, its ease of use and reliable service and support."

About Corero Network Security

Corero Network Security is a leading global provider of Network Intrusion Prevention Systems (IPS) and Distributed Denial of Service (DDoS) attack defense solutions that enable enterprise organizations to protect their critical online assets against risks associated with network-borne cyber threats. Corero, formerly Top Layer Security, is headquartered in Massachusetts, U.S. with sales and services support worldwide. www.corero.com.

Corporate Headquarters

1 Cabot Road
Hudson, MA 01749
Phone: +1.978.212.1500
Fax: +1.978.212.1600
www.corero.com

EMEA Headquarters

No.1 Cornhill
London
EC3V 3ND
Phone: +44 (0) 203 427 3407

To purchase Corero Network Security solutions, please contact your Corero representative at **1.978.212.1500** or authorized reseller.