

Brady Distributing Company Says It's "Game Over" for Malicious Content with Corero IPS

Summary

Industry: Amusement games and vending machines

Challenge: To implement a low latency, set-it-and-forget-it security solution that would block malware and other cyber threats, including distributed denial of service (DDoS) attacks

Solution: Corero's IPS

Results: The system has reduced security alerts down to one or two a month, virtually eliminating the malware problems at remote offices.

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

Since 1944, Brady Distributing Company has been a family owned and operated business that provides sales and services of jukeboxes, amusement games and vending machines. Based in Charlotte, North Carolina, Brady has three additional locations in the U.S. that give the company market reach spanning from Texas and Oklahoma, to the East Coast, and into the Caribbean and South America. Brady Distributing has about 120 employees and is the second largest company in its vertical market, serving customers that range from individual homeowners with arcade-style game rooms to large amusement companies like Incredible Pizza and Walt Disney World.

The Challenge

Brady Distributing conducts its business with heavy reliance on the Internet, which means malware, viruses and Denial of Service (DoS) attacks are disruptive.

Rick Baird is the manager of Brady Distributing's IT department. He resides in Charlotte and has responsibility for the computer systems in the Memphis, Orlando and Miami offices as well. "Since our remote offices are relatively small, we use an MPLS network and Citrix gateway to bring them into our main network in Charlotte. That's where we host our business software and applications such as email," says Baird. "With all of our communications and business transactions from the remote offices going over the Internet, I am always concerned about security and availability. I need to have security at the same level all across the organization without impacting performance."

Lack of visibility into what was happening on his network – and especially on the remote PCs – was a big problem for Baird. "It seemed like the field office PCs were always gathering viruses and malware. Even with anti-virus software installed, the bad stuff was still getting through, and I couldn't oversee what was going on." The company has a firewall for its MPLS network and a content filtering appliance that allows Baird to block undesirable websites, but these didn't provide enough layers of security. In particular, the content blocking by domain name proved insufficient. "As soon as I'd block one site with malicious content, another one would pop up," says Baird. Malware and viruses were still getting through, threatening the business and consuming the IT department's resources to remediate the problems. Baird decided to add an Intrusion Prevention System (IPS) to the company's line of defense.

The Solution

Baird discovered the Corero IPS when attending a trade show. "I watched a live demonstration and could see how easily hackers can get through a firewall. It left me feeling very vulnerable. If they could get through that firewall so quickly, they could get through mine as well. I determined that we needed to have an IPS to be ahead of the curve," says Baird.

He considered competitive IPS products from Tipping Point to Sourcefire but selected Corero's IPS solution for its differentiated 3 Dimensional Protection. Not long after the eye-opening demonstration at the trade show, Baird placed the order for a Corero IPS 5500 appliance to install in the company's Charlotte data center.

"It only took an hour to install the IPS and get it up and running. Straight out of the box, Corero's differentiated solution had a lot of capabilities that the other IPS vendors' products just didn't have, such as protection against Distributed Denial of Service (DDoS) attacks, stateful firewall filtering and protection against Botnet attacks. Everything was there when the device was plugged in," said Baird.

The next step was to customize the configuration for Brady Distributing's environment. "Corero technicians stayed in constant contact with us for the next four to five days in order to make adjustments as we saw things coming in," explains Baird. "Since the initial installation and tweaking, the system has been running by itself. We apply the needed updates and advisories that come out, and beyond that, no other changes have been needed. It just works."

Baird has been greatly impressed by Corero's approach to protection – especially the ability to defend against constantly evolving threats. With his IT department being lean, he needed a protection system that would be automatically updated when new threats emerged, including zero-day attacks. Corero's Update Service keeps threat information current so that Brady Distributing's network is always protected. "We really appreciate getting the regular updates that Corero sends out. In my opinion, this keeps my organization ahead of the curve by always keeping us up to date."

The ability to protect against malicious content was especially important to Baird, since malware was a real pain point for the company. The Corero IPS provides broad and deep protective measures to reduce the risks and losses of compromised computers by eliminating the threats as they traverse the IPS on the network. Threatening network traffic doesn't even reach its intended targets: the servers and PCs on Brady Distributing's network. Corero also has a unique second level validation architecture that gives the device the ability to identify remote exploits on the network traffic. The IPS makes extensive use of protocol and file validation, inspecting all the packets not only for the protocols that carry the network traffic but also the payloads being carried by those protocols. Data validation modules inspect payload files with file-format-specific rules, trapping the kind of malicious content that used to plague Brady Distributing's systems.

The stateful firewall filtering is another dimension that provides peace of mind. It prevents undesired access to Brady Distributing's business-critical systems, applications and data. The Corero IPS acts as a complement to the company's previously existing firewall to give an extra layer of protection.

The IPS' centralized management system gives the IT department unprecedented insight into the state of network security. "Now we're able to monitor our systems and look at the attacks coming in," says Baird. "More importantly, though, we know those attacks aren't advancing into the network and we don't have to worry about them."

Another important feature of the Corero IPS is its low latency. "With our remote offices connecting back to the data center in Charlotte, it's absolutely critical that we have the Internet connections and all security systems up and running as fast as possible so that everyone can work as smoothly as possible," according to Baird. Even with the IPS being in line with the Brady Distributing network, there is no latency to cause a slowdown or any delays.

The Results

Brady Distributing's infrastructure is secure and Baird said he couldn't be more pleased with the results. "The issues we had prior to installing this solution have virtually disappeared," says Baird. "Now we get one or two notifications a month." This has really freed up the IT department to focus on helping run the business rather than remediating issues such as spyware and malware.

"Our network is more secure than it ever was before," according to Baird. "I don't have to worry about it. This IPS has cut down on the malware, spyware and intrusions we were experiencing. It has made my job a whole lot easier and my network a whole lot safer and the performance is outstanding."

Baird praises the installation help he received from Corero. "The Corero people are as good as anybody I've ever worked with. They really helped us with the configuration work, but I have to say that we've never needed them for technical support issues. It is such a sound product that we simply haven't had any."

Looking toward the future, Brady Distributing will soon host a new website to handle more online orders. "About five percent of our business comes from online orders today, but we expect that to grow to 15 to 20 percent of our business once the new application is in place. This business would be worth millions of dollars to the company," says Baird. If something like a DDoS attack were to disrupt access to the website, Brady Distributing could lose significant revenue. This just isn't a concern, though. "SYN floods are what we get the most of, but the IPS allows me to block a lot more stuff on top of what a regular firewall will do and what my anti-virus software does," says Baird.

He's happy to declare, "Since we installed this IPS, my job of securing the network has gotten so much easier. Corero provides us with the protection we need and it keeps us ahead of the curve."

About Corero Network Security

Corero Network Security, formerly Top Layer 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 on-line assets against risks associated with network-borne cyber threats. Corero 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 your authorized reseller.