

Applied Innovations Stands Guard Over 35,000 Client Websites with Corero IPS

Summary

Industry: Windows web hosting

Challenge: Protect clients and their 35,000 websites against sophisticated new exploits, including zero-day attacks and DDoS attacks that threaten the business of e-commerce companies.

Solution: Corero's IPS

Results: The system protects Applied Innovations' clients against malware and DDoS, while its low latency allows production traffic to flow unimpeded. Ease of use means very little management, and use of security reporting features helps inform and retain clients.

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 network architecture

Web hosting provider Applied Innovations specializes in hosting on the Windows server platform for thousands of clients and some 35,000 websites. Boca Raton, Fla.-based Applied Innovations was founded in 1999 with the goal of providing the technology and resources that businesses (particularly SMBs) require to make them competitive and successful at a cost-effective price. Applied Innovations views its relationship with its clients as a business partnership, as the success of one is inextricably bound with the success of the other. Strong security against the myriad threats, from malware to distributed denial of service, is critical to thriving online companies, and critical to the web hosting provider that is responsible for that security.

The Challenge

Companies entrust their business to Applied Innovations. And, as a web hosting provider, Applied Innovations' business depends on keeping their customers' websites and sensitive corporate information secure against attack from the automated and targeted cyber attacks that plague e-commerce across the Internet.

"We are responsible for the security of some 35,000 websites," says Dan Farrell, Applied Innovations' Director of Network Operations. "All have the potential to be hacked."

Farrell was concerned that Applied Innovations needed an additional layer of security to protect its customers in an increasingly dangerous online environment. Cyber criminals are using automated tools to incessantly scan potential target websites for vulnerabilities and launch damaging exploits when they find them. Well-publicized targeted attacks, often exploiting previously unknown or zero-day vulnerabilities, have successfully breached high-profile companies.

In addition to high-profile attacks (such as RSA, Aurora attacks against Google, Adobe and others), smaller companies are being attacked in large numbers, sometimes as chance targets of opportunity, sometimes as chosen victims, because they are generally less secure but offer big payoffs. The business accounts of many SMBs have been cleaned out to the tune of tens, even hundreds of thousands of dollars. The risk-reward ratio is very high.

"We noticed some intrusions, and hackers are coming up with new exploits and compromises that can have a huge cascading effect in our operation," says Farrell. "There was a gap in our security."

“Our existing security measures worked well for what they were designed to protect, but we were missing deep packet inspection to look for exploit code and malicious code, especially zero-day exploits.”

Farrell was also concerned that some of those thousands of client websites might themselves be compromised and become malicious hosts, serving malware to visitors and customers.

“That would be embarrassing and a huge security problem,” Farrell observes.

There's more. E-commerce sites, such as those of many of Applied Innovations' clients, need their sites to be always available and responsive to serve their online customers. A distributed denial-of-service can be disastrous. A slow site – or a site that is down completely – can cost a company thousands, potentially even millions of dollars depending on the type of business and the duration of the attack. Frustrated customers will simply go to another site to spend their money; they may be sufficiently discouraged that they never come back. DDoS is often perpetrated by unscrupulous companies looking for a competitive edge, or cyber-criminals who extort money from online businesses, such as e-commerce and online gaming sites, under threat of launching a DDoS attack.

“DDoS is very much directed at our clients,” Farrell declares. “They are financially motivated attacks – classic extortion.”

“It's important to surgically remove malicious traffic and keep legitimate traffic flowing. We have the blade [Corero IPS], the surgical weapon of choice.”

*Dan Farrell, Applied Innovations
Director of Network Operations*

DDoS is a growing problem – Gartner reports DDoS increased 30% in 2010 and projected continued growth – as attackers have added insidious, hard-to-detect application-layer attacks to their still-potent arsenal of more traditional network-layer flooding techniques. Hacktivist groups, such as Anonymous and LulzSec, launch DDoS attacks against MasterCard, Visa, PayPal and government agencies such as the CIA and U.K.'s Serious Organized Crime Agency. Sony, WordPress and the Hong Kong Stock Exchange are among other victims.

The Solution

Applied Innovations had outgrown its outmoded, open-source based IPS solution that didn't come close to meeting its requirements for performance, detection and keeping up-to-date with threats. “We needed a carrier-class commercial product,” Farrell recalls. Farrell chose Corero Network Security IPS over a TippingPoint product following a month-long live evaluation to see how well they performed and how they integrated with Applied Innovations infrastructure. One of the key capabilities

is that Corero IPS can be deployed in watch mode, which enabled Farrell to see what it detected and would have blocked if it had been set to do so. This allowed Farrell to observe the IPS behavior without the risk of false positives, especially since Applied Innovations' requirements as a web hosting provider for myriad customers required very precise filtering.

“DDoS is very much directed at our clients. They are financially motivated attacks – classic extortion.”

Dan Farrell, Applied Innovations

“We have many customers, and they have to be segregated for security, for PCI compliance,” he notes. “We have unique, granular needs for protection, to be granular with rule sets.”

Corero's low latency – the best in the industry – was a critical factor in Farrell's decision. Because IPS is deployed in line, it must be transparent on the network, not “a bump in the wire.” Corero IPS met all Applied Innovation's requirements for deep packet inspection filtering and detection without any lag on the network. For example, a couple of Applied Innovations' international clients maintain extremely high performance to the Internet through direct connections with their carriers to reach their sites hosted with Applied Innovations. Corero IPS has kept up without issue.

As e-commerce companies, instantaneous response is crucial for a large percentage of Applied Innovation's clients, whose business depends on happy customers who can quickly get the information they need, make their purchases and move on. If the website is sluggish, the customer is gone.

“Our clients have a very low threshold for delay,” Farrell says. “If you are buying a pair of shoes online, and the site's not coming through properly, you are going to go to another site.” Farrell also appreciates that Corero IPS will continue to pass traffic in the event it somehow fails, so that business will continue uninterrupted. This is unlikely, given Corero IPS' very high reliability, with a 20 to 30 year mean time between failure and hot-swappable power supplies and fans.

Corero's integrated DDoS defense capability is unique among IPS products, addressing Farrell's concern about attacks against Applied Innovation's clients. Corero IPS uses a patented DDOS detection algorithm and behavioral analysis to identify attack traffic and mitigates DDoS through its traffic rate-limiting capabilities. Corero IPS is effective against both traditional network-layer floods and the newer, more insidious application-layer attacks. Thus, Corero gives Applied Innovations – and its customers – protection against both malware-based exploits and crippling DDoS.

Farrell also insisted on an easy to use, familiar interface to make management simple and intuitive. “You need an interface that makes sense to someone who understands networking,” he says. By contrast TippingPoint “looked radically different. It's

critical that when you're dealing with issues on the fly, you don't want to have to mentally change gears."

In the evaluation, Corero IPS proved its worth for detection/prevention against the attacks and exploits that threaten 35,000 Applied Innovation websites. Malicious traffic is detected and stopped before it reaches its intended targets, thanks to Corero's unique second-level validation architecture that complements its signature-based detection engine. The IPS makes extensive use of protocol and file validation, inspecting all packets not only for valid protocol behavior and the payload files with file format-specific rules, but also detecting the sophisticated attacks and zero-day exploits which are of such concern to Farrell.

"It's important to surgically remove malicious traffic and keep legitimate traffic flowing," he says. "We have the blade, the surgical weapon of choice."

The Results

Thanks to Corero IPS, Applied Innovations customers are more secure today, and, thanks to its strong reporting capabilities, they know it.

"We like the ability not only to see things in real time on the unit, but use the reporting features to watch trends over time and do security reviews for our clients," he says. "We show them how we blocked these attacks. We communicate what we are protecting and how they would be vulnerable otherwise."

"Most other providers can't meet that level. It helps keep our clients with us."

Corero also exposed the dangers coming from within Applied Innovation's networks. Prior to deploying Corero IPS, Farrell and his staff viewed most security threats coming from external attacks. Because Corero IPS monitors and filters both inbound and outbound traffic, outgoing attack traffic and communications with command-and-control servers can be observed. "It was a real eye-opener to see what your internal network is capable of from a security perspective," Farrell says.

"We use the reporting features to do security reviews for our clients. It helps keep our clients with us."

Dan Farrell, Applied Innovations

He is also happy with Corero's "personalized approach to support as opposed to being just a number."

About Corero Network Security

Corero Network Security (CNS:LN) is a leading global provider of Network Intrusion Prevention Systems (IPS) and Distributed Denial of Service (DDoS) defense solutions. Enterprise organizations rely on Corero 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 offices 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.

Copyright 2011 Corero Network Security, Inc. All rights reserved.
