

# Journal Register Company Delivers News in Real Time with Corero's IPS

## Summary

**Industry:** Publishing

**Challenge:** To implement a secure and reliable solution that could block existing and emerging cyber threats -- including advanced types of malicious activity, such as botnets and other malware, as well as Distributed Denial of Service attacks.

**Solution:** Corero's IPS

**Result:** Corero Network Security stopped a DDoS attack that had hit its systems and bypassed the incumbent firewall technologies dead in its tracks.

## Key Benefits

- Stops advanced threats
- Lowest latency, superior throughput
- Reliable, purpose-built hardware
- Fast, easy deployment
- Blocks botnets, spyware, viruses and other malware
- Compatible with cloud-enabled infrastructure

*As a trusted provider of local news and information to 992 communities in 10 states, the Journal Register Company is one of the largest newspaper publishers in the United States. With 324 multi-platform news products that include Web and video offerings as well as print, the Journal Register is a digital-first organization serving an audience of 15.8 million people every month. The Journal Register's written articles and video streams deliver timely, accurate local information around the clock to residents of Connecticut, Maine, Michigan, New Hampshire, New Jersey, New York, Ohio, Pennsylvania and Vermont.*

## The Challenge

In the process of transforming itself from a legacy print-only newspaper publisher to a 21<sup>st</sup> century digital-first news organization, the Journal Register Company experienced a network attack. Malware breached existing defenses at one of the company's regional news-gathering locations and began degrading network performance.

At the time, the Journal Register's CTO, Bob Mason, had been with the company only about a month. But, early on, he had identified network security inadequacies and had already engaged an outside firm to conduct an enterprise-wide security audit.

"When I arrived at the company we were using several different brands and versions of firewall technology," says Mason. "But, we wanted to be more proactive about protecting our locations. So, the audit was a starting point for considering how to take a more strategic and standardized approach across the enterprise."

Then, midway through the audit, the Journal Register's Michigan location experienced a DDoS [Distributed Denial of Service] attack, significantly impacting the content delivery.

"As a news and information organization, people depend on us," comments Mason. "And, from a business perspective, reliability is our most valuable competitive asset. If we can't provide our audience with real-time content, they'll seek it elsewhere."

Clearly, the Journal Register needed to stop the malicious attack – fast. "It became quite urgent that we provide mitigation," Mason affirms. "And, concurrently, we wanted to adopt the appropriate technology to protect us going forward."

## The Solution

For the Journal Register, the goal was implementing a solution that could handle all kinds of existing and emerging threats – including advanced types of malicious activity, such as botnets and other malware – as well as DDoS attacks. "We wanted a solution that not only addressed the complex threats of today but also came with the intelligence to adapt to the threats of tomorrow," Mason says.

What's more, a solution would need to be cloud-compatible because the company was undergoing an agility initiative which involved migrating its major business applications to several different SaaS vendors. "Since we were moving from primarily in-house infrastructure to a hosted model, it was imperative that a security solution protect our remaining internal network and our connectivity with the cloud," explains Mason.

In addition, low overhead was essential. "We needed a total solution that permitted us to stay lean as an IT organization," Mason says. "We didn't want a security technology that required five or six people just to maintain it."

Fortunately for his new employer, Mason had rigorously evaluated security solutions in his previous position. "At my former company, we'd recently evaluated the major security players," says Mason.

"We had even dropped evaluation units from two vendors in place," he continues. "But, neither of them could stop all of the threats. And, neither of the vendors took ownership when we contacted their technical support staff. Instead, it was a series of 'try this and call us back.'"

So Mason had turned to Corero. He requested a Corero IPS demo unit and placed it in front of the two other solutions. "Corero took ownership from the start," Mason reports. "An engineer brought in the device and didn't leave until all our problems were solved. This included thoroughly training us to use the system."

Given this positive experience, Mason knew who to call when the attack on the Journal Register began. "Although Corero was a very strong candidate, we had planned to go through a regular evaluation process," says Mason. "But the situation required immediate action. So, we decided to partner with a proven leader that had demonstrated the ability to block advanced network attacks in a real-world situation."

Within hours of contacting Corero, help was on the way. "They jumped right in," affirms Mason. "Its team arrived on site quickly and took only a couple days at each location to get the solution running. For us, it was seamless and the whole process was very compelling."

Beyond deploying the units, the Corero technicians studied the Journal Register's infrastructure, analyzed traffic patterns and offered suggestions for improving the company's security approach. "Corero spent a lot of time on knowledge transfer and sharing best-of-breed methodologies," Mason asserts. "This helped us improve the sophistication of our security posture, overall."

## The Results

The initial malicious attack was blocked quickly and within two weeks of contacting Corero, the Journal Register's multiple sites were secured. In place of the insufficient firewalls, Corero's IPS

devices were installed in four locations: the company's greater-Philadelphia headquarters, its disaster recovery site and the regional offices in Connecticut and Michigan.

Since deployment, no malware has breached the Journal Register's defenses and the Corero IPS devices have operated with little or no intervention. "Now our network staff can sleep at night," Mason comments.

Indeed, Mason says the Corero IPS devices are relatively hands off and updates and upgrades occur automatically. These capabilities save the Journal Register untold resources. "Network attacks are ever-changing and increasingly complex," he notes. "It's important to us that we have a multilayer, multithread solution that can learn and adapt quickly to address new threats. And, it's critical that updating not only occurs automatically, but also that it happens in real time to keep us protected."

In addition, Corero's ongoing training opportunities have helped the Journal Register evolve its security posture. "We learn about emerging threats, how to analyze traffic and strategies for being proactive," says Mason. "We also hear about the new capabilities that become available as the devices are upgraded and the ways we can maximize their potential."

In fact, Journal Register views continuing education as a best practice because "our IT team was previously unfamiliar with intrusion prevention solutions," says Mason. "Now they understand how to get the most from the technology and they keep their skill sets sharp."

Another best practice will be utilizing the Corero Security Optimization Service, where engineers visit the Journal Register to review network configurations and suggest appropriate security adjustments. "We'll take advantage of the service to ensure we're operating as effectively as possible," Mason says.

In a nutshell, Corero has played a vital role in the Journal Register's successful transition to an agile, cloud-enabled, digital-first content delivery provider.

"Corero has absolutely provided the protection that has enabled us to transform our IT organization and our entire enterprise," he says. "The peace of mind that the partnership has given us is huge."

## 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 enterprises to protect their critical online 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](http://www.corero.com).

### Corporate Headquarters

1 Cabot Road  
Hudson, MA 01749  
Telephone: +1.978.212.1500  
Fax: +1.978.212.1600  
[www.corero.com](http://www.corero.com)

### EMEA Headquarters

169 High Street  
Rickmansworth  
Hertfordshire WD3 1AY  
Telephone: +44.0.1923.897333

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