



CASE STUDY

CNI Defends DDoS Attacks with Corero SmartWall Solution

Established in 1993, CNI is an Internet Service Provider that was formed through a collaboration of 17 Ohio independent local exchange companies (ILECs). CNI has since grown to 21 ILECs and one electrical cooperative, and it now serves communication providers throughout the United States. CNI provides IPPBX Voice Services, Cloud Connectivity, DWDM Services, Dedicated Internet Access, and wide-area network (WAN) transport services to meet the needs of businesses and service providers throughout its coverage area.

CNI is committed to operating its network and service with integrity, and to early adoption of new and innovative voice, video, and Internet access and data applications.

SUMMARY

TYPE OF SERVICE PROVIDER

Premier Operations Support and Development Center for next-generation Broadband Service Providers; Regional Backbone Provider in Ohio and Michigan. Wholesale ISP, Transport Provider

SCALE

Protects 200Gbps of transit

SOLUTION

Corero SmartWall® NTD1100

DEPLOYMENT MODEL

Inline, at the network perimeter

COMMERCIAL MODEL

Value-add (no charge) to end customers



THE SOLUTION

CNI has two SmartWall® Threat Defense System appliances, connected at 100Gbps, to ensure that only clean traffic gets into the CNI network. The appliances are deployed inline at the network perimeter to provide real-time attack mitigation and network resilience. Both appliances have built-in bypass functionality that allows them to be deployed effectively at the edge of their network, without data continuity risks in the event of system maintenance or a failure.

"We looked at many solutions and ultimately chose Corero's SmartWall because we liked the way it reviews and scrubs data, and the fact that it has an optical bypass option in the event of maintenance or failure," said Plaisier. CNI has been a Corero customer since 2017.



CHALLENGE

CNI's network is targeted by more than 1,000 DDOS attacks per month, that very greatly in duration; most are under 15 minutes, some are around a minute, and some last as long as an hour and forty-five minutes. The attack volumes range from 200 Mbps to 15 Gbps. Prior to deploying the Corero DDoS mitigation solution, CNI attempted to manually block DDOS attacks, but that approach was time-consuming, labor-intensive, and not very effective. The only alternative was black-holing/null-routing attacked customers, which would have been unacceptable because that approach blocks them completely, including their legitimate traffic. "We needed a proactive, automated approach to protect our customers from DDoS attacks," said Randall Plaisier, CNI's Chief Technology Officer.



CORERO SMARTWALL AT A GLANCE

- » Surgically and automatically removes DDoS attack traffic, before it reaches critical systems, eliminating downtime, ensuring optimal performance and maximum availability
- » Prevents impact from even the most sophisticated DDoS attacks ranging from volumetric floods, to state exhaustion attacks, at layers 3 to 7
- » Delivers line-rate, always-on distributed denial of service attack protection, in a solution that scales to tens of Terabits per second of protected throughput
- » Delivers comprehensive forensic-level analysis before, during, and after attacks



RESULTS

Prior to implementing the SmartWall TDS solution, the rising number of DDoS attacks were an everyday risk for CNI and its many customers. "Corero has improved our network security by letting us provide Dedicated Internet Access (DIA) without worrying about DDOS attacks on our customers," said Plaisier. "Our DIA is more reliable than others because the SmartWall detects and mitigates attacks immediately and automatically, without impacting network performance. Corero's patented, heuristic Smart-Rule technology effectively mitigates both existing and newly discovered attack types."

Plaisier says that the Corero solution has reduced CNI's operational costs, because "We don't need to take a hard hammer to stop attacks, or assign customer support staff when a DDOS attack is hitting a customer." Furthermore, Corero's SmartWall always-on protection provides CNI with real-time forensic data about the threats. "Our favorite feature of the SmartWall is the ability to see the target IP address, as well as the attack volume and duration, so we can notify our customer, if necessary." Plaisier continued, "We are thankful for our partnership with Corero so we can provide our customers a network connection that is always up for their mission critical devices."



RESULTS FOR CNI

- » No need to blackhole or null route all traffic to a DDoS target
- » Negligible false positives impacting legitimate traffic
- » Maximum levels of service availability are maintained for users, even in the face of a DDoS event
- » DDoS attacks are automatically mitigated locally at each of their PoPs, avoiding the need to backhaul traffic across the network for mitigation
- » Increased staff efficiency resulting from the automatic and accurate protection
- » Increased user satisfaction resulting from the speed and accuracy of protection

About CNI

CNI is an Ohio-based company, formed through a collaboration of 17 Ohio independent local exchange companies (ILECs). After over 25 years of service, CNI has grown its ownership base to 21 ILECs and one electrical cooperative. While still based in Ohio, we have extended well beyond our local service providers to communication providers located throughout the United States. CNI's provides the highest quality communication offering to local providers is found to be an early adopter of new and innovative voice, video, and Internet access and data applications. CNI has added Quality of Service (QoS) and Quality of Experience (QoE) metrics to its traditional voice and IP service offerings. CNI, operates a 24/7/365 Network Operations Center (NOC) and Call Center.

About Corero Network Security

Corero Network Security is dedicated to improving the security and availability of the Internet, through the development of innovative DDoS mitigation solutions. We are the leader in real-time, high-performance, automatic DDoS attack protection, with comprehensive attack visibility, analytics and reporting. Deployed on-premises, hybrid, and in the cloud, we protect thousands of organizations world-wide, across many verticals. The Corero SmartWall® Threat Defense System (TDS) family of solutions utilizes modern DDoS mitigation architecture to automatically and surgically remove DDoS attack traffic, while allowing good user traffic to flow uninterrupted. For more information, visit www.corero.com.

US HEADQUARTERS

Corero Network Security Inc.
293 Boston Post Road West, Suite 310
Marlborough, MA 01752
Tel: +1 978 212 1500
Email: info@corero.com

EMEA HEADQUARTERS

Corero Network Security (UK) Ltd.
St Mary's Court, The Broadway,
Amersham, Buckinghamshire, HP7 0UT, UK
Tel: +44 (0) 1494 590404
Email: info_uk@corero.com

