

CASE STUDY

SMARTWALL PROTECTS THE CORE OF

NIAGARA REGIONAL BROADBAND NETWORK



Municipally owned by Niagara Falls and Niagara on the Lake, NRBN utilizes a fiber-based network to provide connectivity for businesses, organizations and residents of the region with a local community focus.

NRBN operates a carrier-class MPLS network, providing Dedicated Internet services, Private Network connectivity, and Voice-over-IP (VoIP) solutions -- all delivered on top of its 100%, wholly owned, fiber-optic network infrastructure. In addition to commercial network solutions, NRBN is in the early stages of deploying fiber-to-the-home (FTTH) services to residential subscribers across the Niagara Region.

Niagara Regional Broadband Network, or NRBN, is a service provider in Ontario, Canada, that serves the Niagara Region.

> Corero Smartwall at a glance



- » Surgically removes DDoS attack traffic automatically, before it reaches critical systems, ensuring optimal performance and maximum availability.
- » Delivers line-rate, in-line distributed denial of service attack protection, from 1Gbps to 100Gbps per rack unit, in a solution that scales to Terabits per second of protected throughput.
- » Prevents the impact of attacks ranging from simple volumetric floods, to sophisticated state exhaustion attacks, at layers 3 to 7.
- » Delivers comprehensive visibility for analysis and forensics, before, during and after attacks.



"Before Corero, we knew of 1-2 large-scale attacks (greater than 10Gbps) that hit our network each year," says Glenn Hynes, Director of Network Technology and Business Transformation at NRBN. "These attacks had a tremendous impact on NRBN's network. This was above and beyond the constant smaller attacks that impacted customers to varying degrees on a regular basis."

Over the past few years, the company faced an ever-increasing threat of large-scale DDoS attacks against its network, and those of its customers. The mitigation steps that were previously effective could no longer keep up, and several of these large attacks impacted the services NRBN offered to clients.

With the smaller attacks, customers needed to request NRBN to black-hole traffic upstream or create access lists manually to block particular types of attack. In addition, NRBN used manual interventions to detect, trace and mitigate any attacks. *"This meant lost time and irritated customers,"* says Hynes

The company began investigating alternate DDoS products and services in 2019, eventually choosing Corero's SmartWall in 2020, as the best solution to their problems.

"We were talking to numerous vendors but were unable to find an appropriate middle-ground or fit for the size of the organization and type of network we are," says Hynes. *"After some extensive searching online and discussions with industry peers, we discovered Corero. Once the product was demonstrated to us, we saw the potential and realized it was a good fit."*

>Value-added Offering



"The costs involved in adding DDoS protection were a "necessary step to ensure the stability of our network," says Hynes. NRBN's customers can add DDoS protection as a value-add to their dedicated Internet services, with pricing for this protection scaling with the size of their Internet connection.

Given how much the security landscape has changed in the last year, Hynes expects that offering DDoS protection as a service will deliver greater value to NRBN's enterprise customers, while providing an additional source of revenue for the organization.

"At its core, Corero protects the NRBN network and ensures we can always maintain our service levels."

"Corero has provided a robust solution that protects NRBN and its customers from the increasing threat of DDoS attacks."

- Glenn Hynes, Director of Network Technology and Business Transformation, Niagara Regional Broad-band Network

>the benefits

NRBN uses an on-premise version of the Corero SmartWall, in an always-on inline scrubbing configuration. The network has two data center locations (Toronto and Buffalo), where it connects with upstream peers. Network Bypass appliances at each data center add resilience for the upstream connections, with individual SmartWall Network Threat Defense devices that scrub the traffic before it reaches NRBN's Transit Edge Routers. A Corero Management Server is centrally located on the network to monitor and control the solution.

Hynes says attacks now have little to no impact on their services, thanks to the SmartWall integration. "Corero has provided a robust solution that protects NRBN and its customers from the increasing threat of DDoS attacks," he says

The visibility SmartWall provides into the incoming traffic is equally valuable for NRBN, as before they brought Corero into the organization, an attack of any size was unknown to them until the negative consequences were felt. With the insights provided by the SmartWall installation, Corero delivers "peace of mind" to NRBN and its customers. "At its core, Corero protects the NRBN network and ensures we can always maintain our service levels," says Hynes.

With DDoS protection now in place, NRBN plans to further enhance its network security products to ensure that customers are "always on," he adds. "As a society we are dealing with an ever-increasing threat of cyber-attack and, at the same time, we need to be more connected than ever before. NRBN will help mitigate these threats, while ensuring business continuity for its customers."



US HEADQUARTERS  info@corero.com

EMEA HEADQUARTERS  info_uk@corero.com