CASE STUDY

Park Region Brings DDoS Mitigation In-house with Cost-effective A10 Defend

Industry | Service Providers

Serving the Community with Great Connectivity

As a regional provider that has been serving rural residents and businesses in West Central Minnesota since 1906, Park Region Telephone Company (Park Region) is always looking to the future with the goal of ensuring prosperity for its customers and community.

Park Region provides high-speed internet, phone, television, home automation, and professional managed services. Founded as a co-operative, the organization is fully focused on serving its community. Through investment in fiber-to-the-home (FTTH) networks, it is on a mission to transform the region into a technology hub.

Park Region's reputation as a high-quality local communications provider is crucial in achieving this ambition, so when distributed denial of service (DDoS) attacks threatened to derail its customer experience, Network and Plant Operations Manager, Ken Budd, knew he needed to find a robust, cost-effective DDoS attack mitigation solution.

> *Our network is not impacted like it has been in the past. In fact, since putting this in place, we haven't had a DDoS attack that has impacted our network and caused any type of downtime for our customers.*
>
> – Ken Budd
> Network and Plant Operations Manager
> Park Region Telephone Company

Network Solution

A10 Defend

Critical Issues

- Deliver high-quality, reliable connectivity to customers and safeguard its reputation as a trustworthy local supplier
- Detect, prevent, and mitigate frequent and disruptive DDoS attacks
- Reduce reliance on upstream providers for DDoS protection
- Invest the co-operative's funds wisely for maximum benefit to members

Results

- Instant, seamless, and transparent mitigation of DDoS attacks
- Value-added service offered to customers that shortens the sales cycle
- A cost-effective DDoS attack mitigation solution
- Protection against customer churn and loss of reputation

Challenges: Taking Control of DDoS Mitigation

Park Region typically experiences one large DDoS attack every month, alongside a multitude of smaller attacks. These threatened to interrupt customer connectivity and damage Park Region's reputation, potentially resulting in customer losses. The organization wanted to gain greater control over its posture against DDoS attacks, but this posed numerous challenges.

Smaller telcos are typically dependent on their upstream providers to deliver DDoS mitigation, which can cause difficulties.

As Ken explains, "If you're going to depend on your upstreams to provide that type of mitigation, you're going to have to enter into agreements with multiple upstreams because you have got to have redundancy when it comes to your internet drains."

With no in-house DDoS mitigation in place, Park Region was relying on burdensome manual processes. Ken wanted to deploy an active solution that would not only mitigate traffic but also set up a "black hole" and route it to a null zero if the mitigation rate was exceeded.

A key barrier to achieving this was cost. As a co-operative organization, Park Region has a duty to ensure all its technology investments deliver maximum benefit to members. However, most DDoS mitigation solutions are priced beyond the organization's investment capacity: "As a small telco, most DDoS solutions are priced way out of our limit," says Ken. "We just don't have the ability to get into that market and provide that service for our customers."

Nevertheless, the level of risk was rising. Ken continues, "Most companies our size just have to absorb the risk of DDoS attacks, but when it reaches the point that attacks are so frequent and disruptive you can't absorb it any longer because your customer retention rate drops and you start losing customers—and customer experience is affected—that's when you start saying, 'Okay, we've got to figure something out here.'"

Selection Criteria: Cost-effective Integrated DDoS Mitigation

Park Region was already using a DDoS detection solution from a third-party provider, so Ken explored using this provider for DDoS mitigation. However, the proposed cost proved untenable. A10 Networks offered a DDoS mitigation solution that not only integrated with Park Region's existing DDoS detection technology but did so at a price-point that worked for Park Region.

The A10 Solution

Park Region deployed A10 Defend Mitigator to deliver advanced intelligent, automated DDoS mitigation. The solution offers multi-vector DDoS mitigation to defeat growing, volumetric cyber-attacks. A10 Defend is a DDoS defense solution that is highly efficient, operating in a small form factor with low power usage, rack space, and cooling requirements, which combine to reduce OPEX.

The A10 Networks team set up and configured A10 Defend Mitigator to work alongside Park Region's incumbent detection solution, which was a real bonus for Ken Budd.

> *"Not only did A10 come and put it in, the team also helped set it up. They walked us through the process, and we saw the benefits immediately because we had some DDoS attacks in excess of 10GB come in, which is a big deal for us, and you could see that traffic being mitigated," says Budd*

Results

Bringing DDoS mitigation in-house has allowed Park Region to offer value-added services, something that has helped the sales cycle for new business and impressed existing customers.

"It has worked for customer retention," says Budd. We have some larger customers, and we can offer them DDoS prevention as part of our service, so they don't have to go somewhere else. It's just another value-add. I know some telcos would charge for that service but I'm putting it as a value-add to retain the customer."

Since deployment, the organization has seen immediate improvements in performance and visibility, as Budd explains, "We've seen DDoS attacks specific to a customer IP address, and that traffic was mitigated, scrubbed out, and passed through. The customer had no idea anything was going on; however, on our side, we could see what was taking place. So, one of the big benefits to us is that our network is not impacted like it has been in the past. In fact, since putting this in place, we haven't had a DDoS attack that has impacted our network or caused any type of downtime for our customers."

Safeguarding its reputation as a high-quality local supplier is a key benefit of deploying in-house DDoS attack mitigation for Park Region. The organization is keen to promote its new offering to local customers. "As a provider in our local territory, we really hang our hat on the local type of service and encourage people to spend locally and keep those dollars flowing within the community to help enhance it."

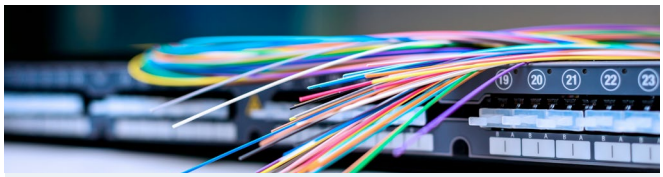
> *"The whole point of a co-operative is to provide a service that meets or exceeds what customers would be able to obtain in a big city...if you're hanging your hat on being local and you lose that reputation, that's a pretty big hit for us," says Budd.*

Success and Next Steps

The A10 Defend has been a tremendous solution for Park Region. Deploying A10 Defend Mitigator is just the start for the company. Next, the organization plans to utilize A10 Defend Detector to detect attacks, effectively providing an even more holistic solution for the regional telco.

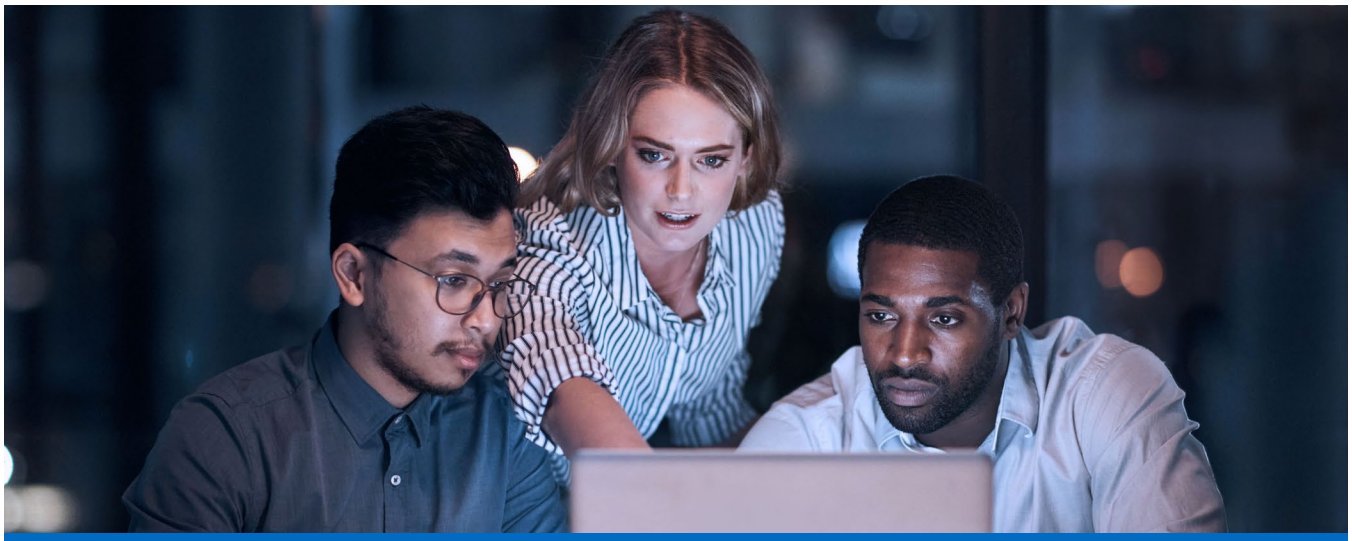
This is one of Budd's key takeaways for other telcos who are considering investing in DDoS protection. "Make sure to put a plan in place to implement the whole solution. Don't just do detector; you definitely want to move into mitigation."

He also advises providers to consider the commercial opportunities of offering complete DDoS protection. "Set some time aside to really get the solution in place and in a way that is going to benefit not just your residential customers or your main traffic, but also think of other solutions that you can resell as an additional revenue stream," emphasizes Budd.



About Park Region Telephone Company

Based in West Central Minnesota, Park Region Telephone Company is a community cooperative that has been providing communication services for rural homes and businesses for more than a century. It is dedicated to securing a prosperous future for the community it supports by turning it into a technology hub. It is investing in network infrastructure including fiber-to-the-home and is committed to delivering a reliable, secure connectivity service for all.



The State of
DDoS Weapons Report

Download Report

Request a live demo and experience the
A10 Networks Difference

Schedule a Demo

About A10 Networks

A10 Networks provides security and infrastructure solutions for on-premises, hybrid cloud, and edge-cloud environments. Our 7000+ customers span global large enterprises and communications, cloud and web service providers who must ensure business-critical applications and networks are secure, available, and efficient. Founded in 2004, A10 Networks is based in San Jose, Calif. and serves customers globally.

For more information, visit A10networks.com and follow us @A10Networks.

Learn More

About A10 Networks

Contact Us
A10networks.com/contact

Part Number: A10-CS-80243-EN-02 NOV 2023