CASE STUDY

BR.Digital Grows Business with Automated DDoS Detection

br.digital TELECOM

Industry | Telecom

BR.Digital serves the communications needs of telecom operators, streaming media services, corporations and regional ISPs with a fiber network that covers 90 percent of the populated areas of Brazil. BR.Digital strives to provide strong security to its customers, with the fastest threat response, to protect the integrity and availability of its customers' data and digital services. Key to protecting against business disruption or fraud is its ability to stop DDoS attacks at scale.

> *We have seen an increase in service orders because of the Thunder TPS DDoS detection solution we deployed."*
>
> — Luis Balbinot
> CTO, BR.Digital

Network Solution

A10 Thunder TPS
A10 aGalaxy

Critical Issues

Needed a faster, more effective DDoS detection and mitigation solution to help you grow your business among government, financial services, health care and other industry sectors.

Results

- Fast, effective DDoS defense protects network availability and safeguards customer against disruption
- Facilitated expanded business in industry verticals with stringent security requirements
- Reduction of BR.Digital's operational expenses by $150,000 with a 3-6 month ROI
- Saved an estimated $100,000 to $500,000 over time with A10 Networks solutions

Challenge: Protect Against Increasing DDoS Attacks

As the pandemic accelerated digital transformation and internet use, so have cyberattacks. DDoS attacks of all kinds are surging, and globally, DDoS weapons have almost tripled in two years.

Protecting customers against these devastating attacks was a top priority for BR.Digital — and a requirement to win new business across government, financial services, and health care organizations.

> *"To bid on government contracts, we needed to meet very strict anti-DDoS requirements."*
>
> *— Luis Balbinot, CTO of BR.Digital*

BR.Digital relied on an in-house DDoS detection mitigation technique, combining an open-source tool to monitor traffic for anomalies, and then when malicious traffic was detected, diverting it to a third-party scrubbing center to be cleaned and returned. As DDoS attacks grew in severity and sophistication, this approach was too reactive, adding latency to the customer experience — and it increased the workload of the network operations team.

To compete for a large government contract, BR.Digital needed a faster, more effective way to stop DDoS attacks.

Selection Criteria

BR.Digital evaluated the leading DDoS mitigation solutions and determined that A10 Networks Thunder® TPS was the best fit for fast, accurate detection and mitigation of a multimodal DDoS attack. The evaluation also determined that Thunder TPS offered the greatest flexibility for customization and integration with BR.Digital's existing management tools, including Kentik for network intelligence.

"The key was the openness and integration of the Thunder TPS solution," says Balbinot.

BR.Digital could also take advantage of A10's consumption-based licensing model, FlexPool®, which allows the company to allocate and re-distribute Thunder TPS capacity across applications and data centers. "Overall, the A10 licensing model stood out compared to other solutions," he says.

The A10 Thunder TPS Solution — a Perfect Fit

BR Digital deployed A10 Networks Thunder TPS 4435 for a fast, effective defense strategy that can pinpoint and block all types of DDoS attacks, including network-layer, application-layer, and ransomware DDoS, across its nationwide network. BR.Digital's backbone has around 35,000 km of fiber optic cables with A10's TPS solution deployed in São Paulo.

A10 Networks' AI-driven Zero-day Automated Protection (ZAP) capability enables Thunder TPS to block a DDoS attack while automatically protecting legitimate users from disruption. ZAP discovers and applies surgical filters without the need for pre-configuration or manual intervention.

BR.Digital uses A10 aGalaxy® to manage Thunder TPS, providing the engineering and operations teams with a single pane of glass to manage, orchestrate, monitor, report, and detect DDoS attacks and defenses. With aGalaxy and the multitenancy capabilities of Thunder TPS, BR.Digital's customers can have direct visibility into a DDoS attack and mitigation, with these reports underscoring the value of the mitigation service.

Brazil Area Coverage

Results

Grow Business with Automated DDoS Mitigation

In the year 2022, the industry has seen some of the largest attacks in history, disrupting communications and critical infrastructure around the world. Stopping a DDoS attack has never been more important.

With Thunder TPS, BR.Digital can automatically stop all known DDoS attacks, protecting customers against this escalating threat and safeguarding network availability. With intelligent DDoS detection, BR Digital is well-positioned to win more business among government, financial services and other organizations that have stringent security requirements.

> *"Potential customers see us differently now that we have a portfolio of well-known customers that are satisfied with our anti-DDoS solution," says Balbinot.*

Maintain Data Privacy

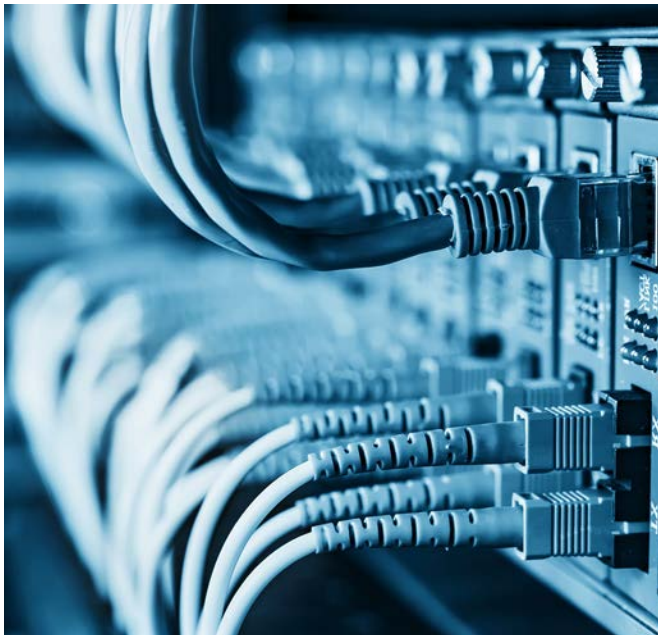
Nor is there concern with redirecting customers' sensitive data — especially for customers in financial services and health care — to a third-party scrubbing center. With Thunder TPS, BR Digital can mitigate application-layer attacks without diverting traffic outside its data centers, adding latency and incurring charges from a third-party scrubbing service.

"Most government and financial services customers require an in-house solution and don't allow the use of third parties for DDoS mitigation," says Balbinot. "We have seen an increase in service orders because of the Thunder TPS DDoS solution we deployed."

Increase Operational Efficiency

Automated detection and mitigation of a DDoS attack reduces high-pressure incident response, minimizing the workload and stress on the network operations team. That efficiency contributes to the ROI of BR.Digital's DDoS mitigation service offering.

Using Thunder TPS for DDoS mitigation also enables the customer to forego the cost of using a third-party scrubbing center, saving the company $100,000 to $500,000 USD over three years, notes Balbinot. He also says that BR.Digital anticipates a quick 3-6 month estimated ROI on its Thunder TPS investment.

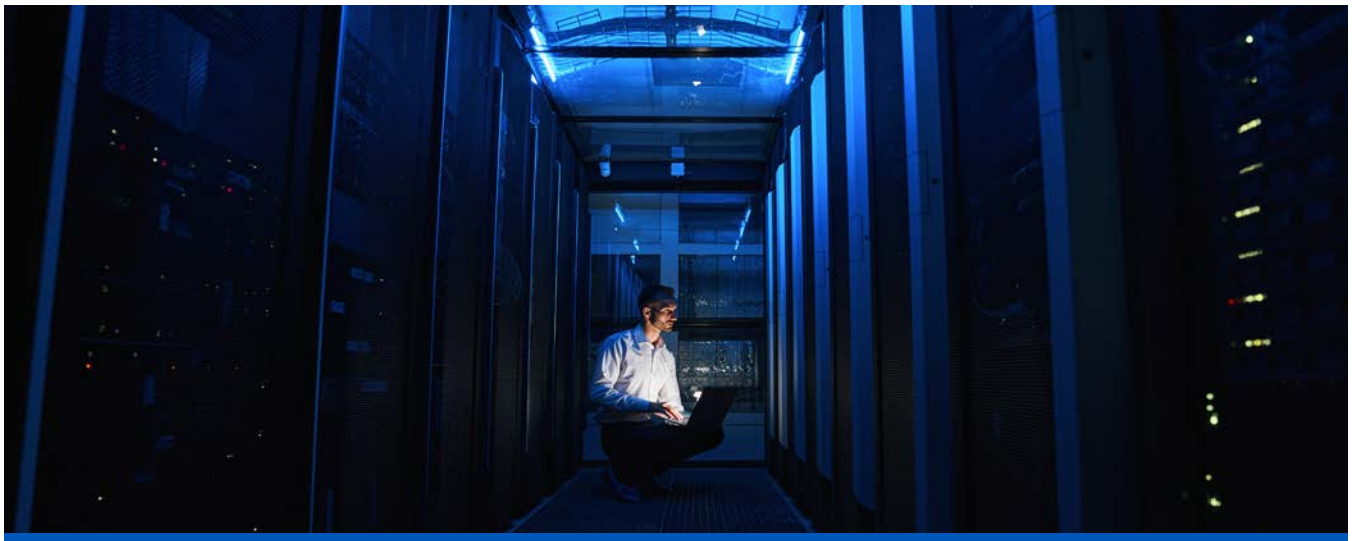


Success and Next Steps

Beyond winning new corporate and ISP customers, a secure network foundation positions BR.Digital to sell other services, such as IP transit, data center, and SD-WAN. And that is good for the company's future.

About BR.Digital

A trusted service provider since 1995, BR.Digital serves the communications needs of telecom operators, streaming media services, corporations and regional ISPs with a network that covers 90 percent of Brazilian territory and nine highly available, secure data centers.



Find out how to manage
IPv4 exhaustion using CGNAT

IPv6 – Are We There Yet?

Download eBook

Request a live demo
and experience the

A10 Networks Difference

Schedule a Demo

About A10 Networks

A10 Networks (NYSE: ATEN) provides secure application services for on-premises, multi-cloud and edge-cloud environments at hyperscale. Our mission is to enable service providers and enterprises to deliver business-critical applications that are secure, available and efficient for multi-cloud transformation and 5G readiness. We deliver better business outcomes that support investment protection, new business models and help future-proof infrastructures, empowering our customers to provide the most secure and available digital experience. 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-80227-EN-01 Nov 2022