MAZEBOLT

Case Study

A Financial Service Provider Slashes DDoS Vulnerability to Under 15%

The client: A leading financial service provider in North America offering a range of digital financial services to its customers, including investment, mortgage, and retirement planning.

Realizing true DDoS exposure

Having suffered a barrage of attacks and major business disruption, the client chose MazeBolt to conduct its annual red team testing in 2021. During the test, the client discovered that it was vulnerable to 50% of the attack vectors tested. Since the red team test was limited and included only 1-3 targets and up to 15 attack vectors, it was an insufficient method for testing the effectiveness of its DDoS protection.

Key Takeaways

Challenges:

- Delivering uninterrupted digital services to its customers
- Limited effectivity of red team testing
- Lack of visibility into a dynamic DDoS attack surface

Solution:

- Implemented RADAR™ testing

Impact:

- Reduced 50% exposure to less than 15%
- Delivered uninterrupted availability of its service to its users
- Changes in network configuration are now validated without operational disruption

Scaling testing and protection

Realizing the severity of their DDoS exposure, the client understood the need for continuous testing and remediation. Since only MazeBolt's RADAR testing could test and remediate these vulnerabilities on a continual basis, the client implemented the solution, being able to expand its range of performing thousands of tests over 140 attack vectors and a larger number of targets.

Closing the remediation loop with dramatic results

With MazeBolt's analysis and remediation plan in hand, the client was able to then work with its DDoS protection vendor to close severe vulnerability gaps, dramatically reducing its risk.

Once the remediation changes were implemented the client achieved the highest level of business continuity and DDoS readiness. Most importantly, they now have a tool to validate any changes in network configuration with zero operational downtime.

.

> **"*Now that we are aware of the vulnerabilities in our environment, we will continue to use RADAR testing to remediate and close vulnerabilities."***
>
> **COO,** Leading North American Financial Services Provider

About MazBolt

MazeBolt is pioneering a new standard in testing DDoS vulnerabilties that provides enterprises with full attack surface coverage. Its vulnerability solution, RADAR^{TM} testing, continuously observes tens of thousands of potential DDoS attack entry points, identifying how attackers succeed in bypassing existing mitigation systems. The solution's autonomous risk detection allows cybersecurity teams to go beyond traditional DDoS testing by continuously detecting, analyzing, and prioritizing remediation across the network with zero operational downtime. Global enterprises, including financial services, insurance, and governments rely on MazeBolt for full visibility into their DDoS security posture. For more information visit: **www.mazebolt.com | info@mazebolt.com**.