MAZEBOLT

Case Study

Eliminating DDoS Mitigation False Positives

The client: a global financial organization that is committed to providing reliable services and tools to its account holders.
Setting up and using the company's services is easy for customers, but behind the facade lies a complex, secure, and highly intelligent platform with intricate applications and networks working seamlessly.
That is, until a single incident spiraled into a hazardous DDoS attack, resulting in legitimate customers being blocked from services.

Key Takeaways

Challenges
- Understanding true DDoS exposure and risk.
- Effectively securing rapidly expanding online services.

Solution
- Implemented RADAR™

Impact
- Drastically reduced risk from 48% to 2% (24x risk reduction).
- Continuous DDoS testing.
- Elimination of False Positives.
- Achieved additional ROI on DDoS protection investments.

The Challenge: Mistaking Legitimate Requests for DDoS Attackers

The client added new services to increase sales and customer engagement for their merchants. One of the applications inadvertently sent customers a push request, resulting in a flood of legitimate responses from them.

Their automated DDoS protection solution mistakenly identified the legitimate request as a DDoS attack and end-users were blocked. Thousands of customers were denied access during this unfortunate event and damage control took a heavy toll on the company's resources and reputation. Going forward, they wanted to ensure that their DDoS protection could keep up with the dynamic pace of change introduced to their online services by the digital transformation without causing false positives.

The Solution: Automatic Identification of Legitimate Requests

MazeBolt RADAR™ empowered the client to test and identify protection of legitimate requests automatically, continuously, and non-disruptively. Being protection services agnostic, RADAR can be added to any existing protection solution to achieve full visibility into legitimate requests blocked towards each web-facing IP/target in its network environment.

By harnessing RADAR's findings, the client worked with the DDoS protection vendor to fine-tune its DDoS protection configuration. By continuously validating its assets against both legitimate traffic and malicious DDoS attacks, two things happened:

1. Minimized false positives – RADAR's insights helped configure DDoS protection for maximum resilience, ensuring no legitimate traffic is being blocked.
2. Maximized continuous DDoS resilience – RADAR continuously tested, identified, and triaged DDoS vulnerabilities, preempting potential DDoS exposures and effectively eliminating risk.

The Benefit: Achieving True DDoS Resilience

With RADAR, the customer's CISO gained visibility into DDoS vulnerabilities to proactively secure online services, regardless of any changes their digital transformation process requires. This visibility is achieved with a few simple steps and includes an easy-to-use interface, clear reports, and remediation plans and objectives. RADAR is quickly deployed and added to any existing DDoS protection solution an organization has in place. Security teams can now focus their efforts on prioritizing DDoS vulnerabilities, saving valuable time and budgets, and achieving true DDoS resilience.

> "MazeBolt RADAR gave us real-time insight into our DDoS exposure and better manage our online services. Now we have actual DDoS visibility."

CISO, Global Fintech organization.

About MazeBolt

MazeBolt is pioneering a new standard in achieving DDoS resilience by providing enterprises with non-disruptive full online services coverage. RADAR™, an industry-first solution, continuously tests tens of thousands of potential DDoS attack entry points, identifying how attackers succeed in bypassing existing protection systems. MazeBolt RADAR's autonomous risk detection allows cybersecurity teams to go beyond traditional DDoS testing to uncover blind spots in their protection layers by continuously testing, analyzing, and prioritizing remediation with zero operational downtime.

Global enterprises, including financial services, insurance, and governments rely on MazeBolt for full visibility into their true DDoS security risk.