



CASE STUDY

Payment Service Provider Eliminates DDoS Mitigation False Positives

Industry: Financial Services

►► Overview

The client is a global Payment Service Provider 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.

Customer Benefits

- ✓ 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 Traffic for DDoS Attacks

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 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.

▶ Our Solution:

Automated DDoS Vulnerability Identification

MazeBolt RADAR™ empowered the client to test and identify protection of legitimate requests automatically, continuously, and nondisruptively. 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 network configurations. By continuously validating its assets against both legitimate traffic and malicious DDoS attacks, two things happened:

- **Minimized false positives** – RADAR's insights helped configure DDoS protection for maximum resilience, ensuring no legitimate traffic is being blocked.
- **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 client 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.



“MazeBolt RADAR gave us real-time insight into our DDoS exposure and allowed us to better manage our online services. Now we have actual DDoS visibility.”

-CISO, Global Payment Service Provider

About MazeBolt

RADAR™ by MazeBolt ensures business continuity for global enterprises by validating their DDoS defenses – without the need for maintenance windows. RADAR's patented technology continuously runs thousands of nondisruptive simulations, allowing organizations to identify and remediate critical vulnerabilities in their DDoS defenses and configurations. This results in measurable reduction in DDoS risk and stronger regulatory compliance – while preventing the operational, reputational, and financial damages caused by DDoS attacks. Learn more at: www.mazebolt.com