MAZEBOLT



CASE STUDY

Global eCommerce Platform Eliminates DDoS Downtime

Industry: Financial Services

The Customer

The customer is an international ecommerce platform that was struggling to deal with recurrent, damaging DDoS attacks. At the time, the customer's static mitigation policies were limited to rate-based and traffic filter strategies.

Although the customer was unable to mitigate the damaging attacks, their technical teams initially were unwilling to consider adjusting their mitigation policies, and were resistant to implementing more sophisticated mitigation tactics. The reason for their hesitation was due to concern about false positives that could impact legitimate traffic and customer services. In reality, the existing mechanisms were already leading to dropped customer transactions.

Customer Benefits

- Eliminated the recurrence of damaging DDoS downtime
- Improved the internal processes that validated readiness of DDoS defenses
- Improved the effectiveness of deployed DDoS protections while eliminating false positives
- Enabled a measurable reduction in DDoS risk - shared with senior management
- Met all necessary regulatory requirements through continuous testing and reporting of findings

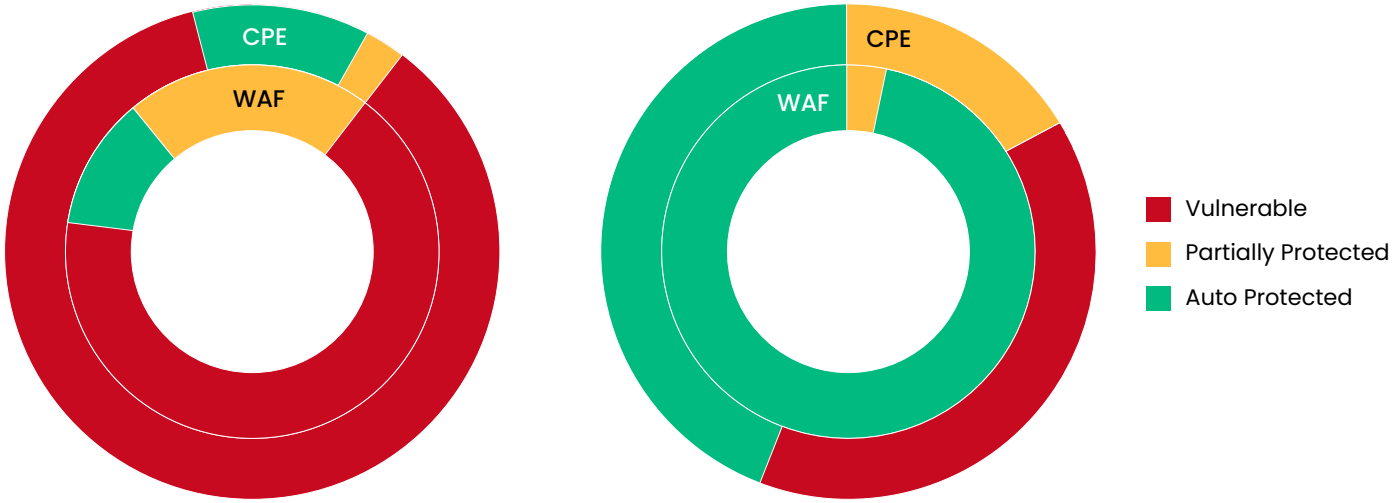
The Challenge

The MazeBolt team deployed RADAR™ to run DDoS attack simulations on the customer's network and discovered that there was an initial 82% vulnerability rate – meaning that the enterprise was only 18% protected from DDoS attacks. However, the technical team was skeptical about this finding, and challenged the results.

Our Solution

The MazeBolt team worked to address the customer's initial concerns and defined a mutual goal: mitigating vulnerabilities while avoiding false positives. RADAR DDoS testing was deployed and detailed reports were generated that provided detailed mitigation recommendations, tailored to their use cases while taking into account the customer's available resources. In addition, each available protection mechanism was mapped to the relevant DDoS vulnerabilities. The customer was able to remediate the most significant issues independently of their DDoS mitigation vendor.

Within a period of three months, the customer was able to dramatically reduce its vulnerability risk from 82% to 27%.



DDoS Vulnerability Before and After RADAR Deployment

Today, the customer continues to use RADAR to validate its DDoS defense. RADAR is deployed as a strategic tool that determines the value and necessity of its deployed DDoS protections. Moreover, as a result of the process that it underwent with MazeBolt's Professional Services, the team was able to discover and mitigate several additional internal procedures that were causing DDoS exposure.

Since deploying RADAR, the customer has not suffered from any DDoS downtime.

> **It was tough to get to this point, but our security team finally understands that we don't need to use volumetric attacks to find DDoS vulnerabilities. And now that we've seen the value that we received from using RADAR, we want to test everything!"**
>
> - Senior Cyber Security Analyst, eCommerce platform

MAZEBOLT

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