



CASE STUDY

# Bridging the Visibility Gap in Days with MazeBolt & F5

Industry: Insurance

## ▶▶ The Customer

A leading insurance company with over 4 million customers was facing frequent, damaging DDoS attacks that led to disruptions and downtime. Their customers experienced repetitive connection issues when using the company's online services. Despite deploying DDoS mitigation solutions and conducting periodic DDoS testing, the company remained vulnerable – and the customer experience was impacted.

The company suffered from:

- Repetitive DDoS downtime
- Service degradation
- Operational and reputational damage

## ▶▶ The Challenge

The company sought to:

- Proactively prevent DDoS attacks
- Maximize ROI from the deployed DDoS security stack
- Gain continuous, full visibility into the DDoS attack surface
- Identify and remediate DDoS vulnerabilities

## ▶▶ Our Solution

All industry-leading DDoS mitigation providers begin with standard protection policies designed for broad compatibility and minimal business disruption. These baseline configurations are intentionally conservative and require environment-specific tuning to achieve optimal protection. RADAR identified configuration gaps that are common in initial deployments and enabled precise remediation aligned to the customer's traffic patterns and risk profile.

### Phase 1: Exposure Discovery & Visibility

MazeBolt worked together with our Preferred Remediation Technology Alliance partner, F5, to give the company full DDoS visibility. Industry-leading vendors like F5 provide extremely powerful DDoS mitigation platforms. For this customer, the deployed policy was generic – and the initial RADAR test showed 86% configuration exposure under standard deployment conditions – i.e., prior to tuning.

## Customer Benefits

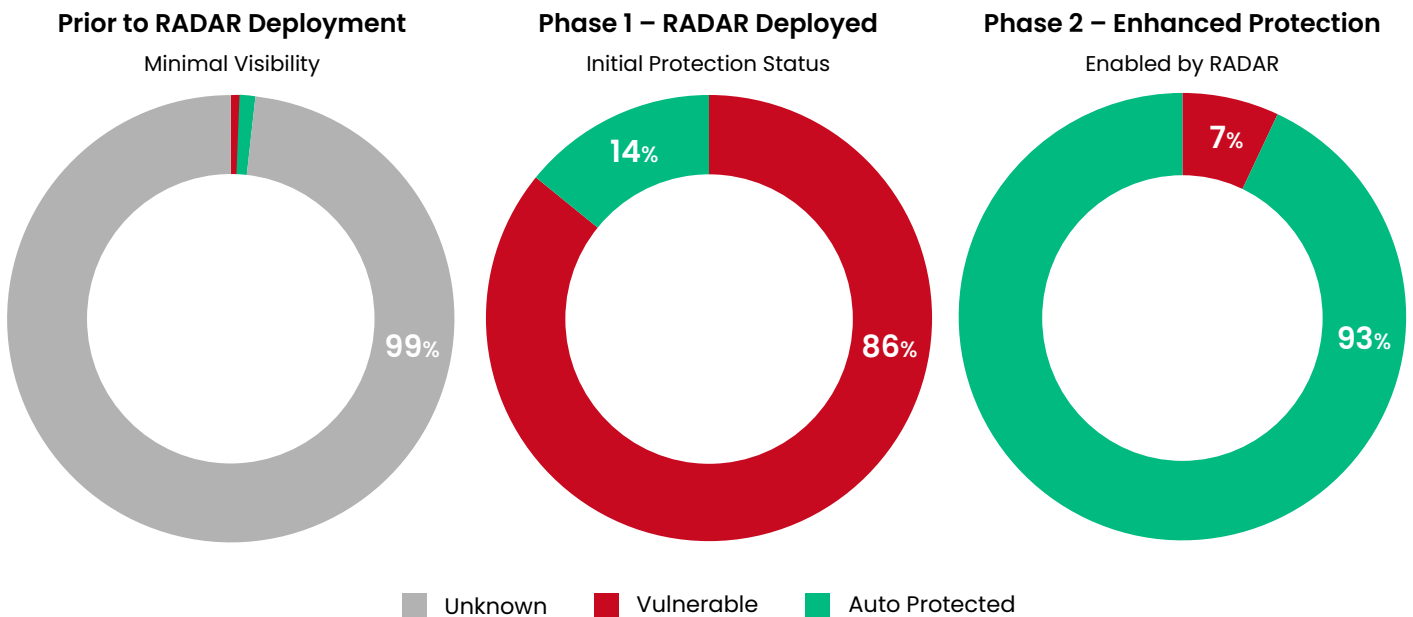
- ✓ Full, continuous attack surface visibility
- ✓ Reduced DDoS risk – from 86% to 7%
- ✓ Remediation achieved in days
- ✓ Zero downtime during and after deployment
- ✓ Fully optimized ROI of existing DDoS systems
- ✓ Eliminated high-cost downtime events

RADAR™ by MazeBolt provided the company with detailed configuration data and generated a full remediation report.

### Phase 2: Automated Protection & Remediation

F5's SOC team incorporated the data that they received from RADAR. They successfully configured F5's XC DDoS protection for optimal protection. This enabled the company to reduce its risk of damaging downtime at record speed.

Overall, with the full visibility and data provided by MazeBolt together with F5, customized configurations were possible that resulted in a reduction of DDoS exposure from 86% to 7% – representing a total risk reduction of approximately 92%. This risk reduction was achieved in days.



Improvement in DDoS Resilience with MazeBolt & F5

This reduction in the company’s DDoS exposure is particularly significant because research highlights a 550% increase in DDoS attacks on the Banking, Financial Services, and Insurance industry, year over year.

The work done jointly by MazeBolt’s Professional Services team and F5’s SOC teams enabled the company to achieve

DDoS auto-protection: the data provided by RADAR testing allowed F5 XC protection to automatically prevent damaging DDoS attacks.

The findings indicated that continuous validation and environment-specific policy tuning must become a common industry-wide standard.



**“The combination of RADAR by MazeBolt and F5’s XC DDoS Protection completely changed the way we manage DDoS risk. For the first time, we had clear visibility.”**

- CISO at Insurance Company

## ►► Deployment Deep Dive

If one universal policy worked for every customer:

- MazeBolt could publish a single vetted configuration
- F5 could ship one hardened template
- No fine-tuning would ever be needed

But in reality:

- Each organization has unique traffic behavior
- Different application architectures
- Different POP distributions
- Different rate thresholds
- Different risk tolerances

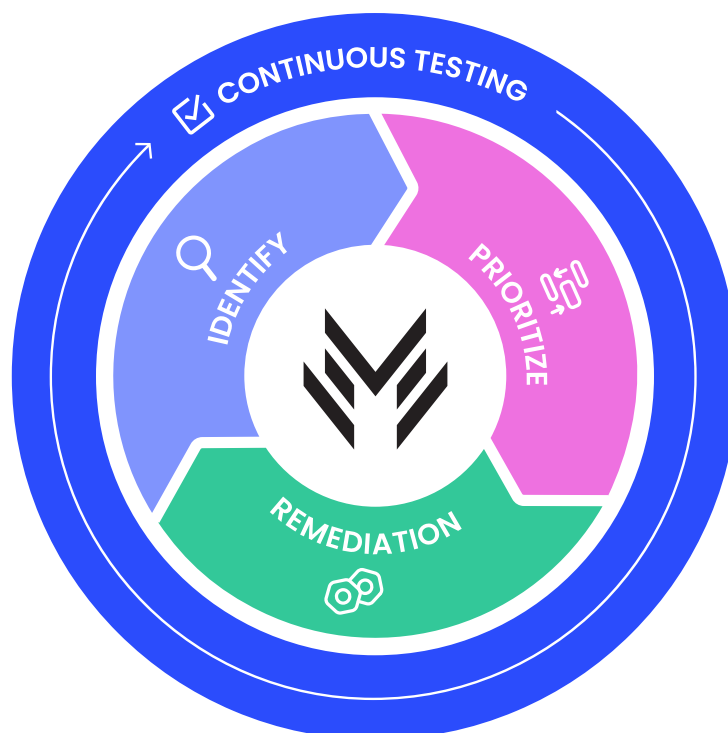
For these reasons, tuning actions were required:

- ✓ Lowering detection thresholds
- ✓ Reducing number of POPs
- ✓ Applying manual rate limiting
- ✓ Leveraging malicious users functionality

To eliminate the company's risk of DDoS downtime, the F5 XC Web Application and API Protection (WAAP) was optimized.

The work done by MazeBolt and F5 enabled the company to align itself fully with the Gartner® framework for Continuous Threat Exposure Management (CTEM) – by providing a comprehensive solution that addresses all five steps of CTEM:

- Scoping, Discovery, and Prioritization (conducted by MazeBolt)
- Validation and Mobilization, which include remediation activities (conducted by F5)



MazeBolt & F5 Support Gartner's CTEM Framework

## 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](http://www.mazebolt.com)