MAZEBOLT

CASE STUDY

European Bank Meets DORA Service Availability Regulations and Avoids DDoS Downtime

Industry: Banking and Financial Services

The Challenge: Maintaining the Business Continuity of Internet Banking

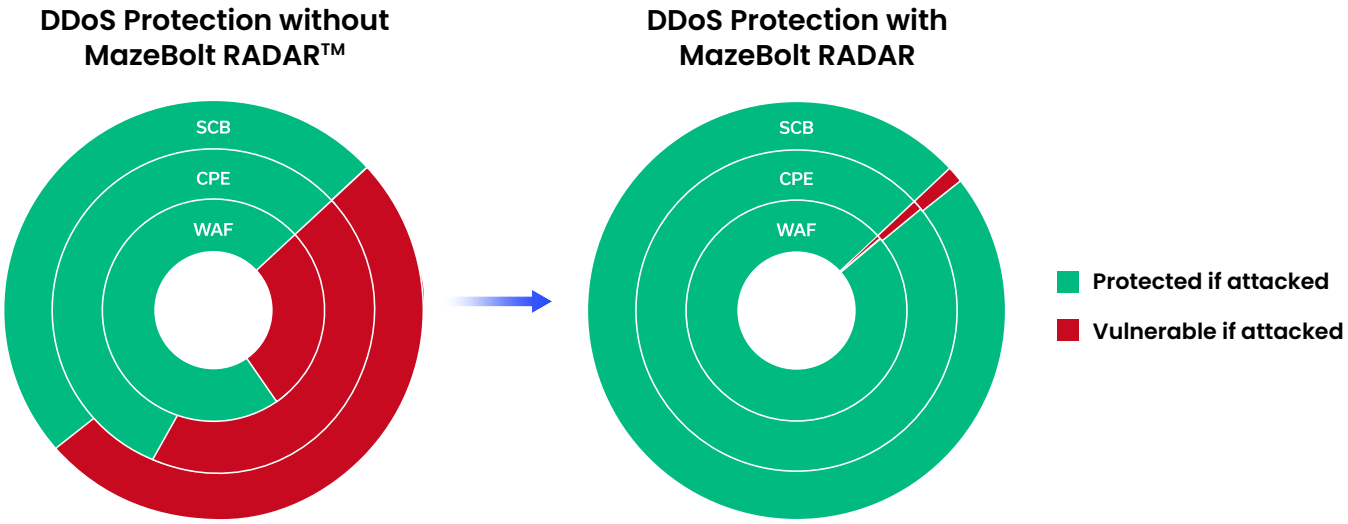
A large European bank was looking for a DDoS vulnerability testing and validation solution that could help them meet the Digital Operational Resilience Act (DORA) and European Banking Authority (EBA) compliance requirements.

It was crucial for them to ensure the business continuity of their online and mobile banking services, which serve as their main channel for all customer-related services.

Customer Benefits

- Improve automated DDoS protection by up to 2X
- No downtime for any critical online services
- Gain necessary data and reporting for DORA
- Save time - for the SOC and IR teams
- Reduce cyber insurance costs

Our Solution: Eliminating DDoS Vulnerabilities with Zero Downtime



Impact of the MazeBolt RADAR™ DDoS Vulnerability Management on the Customer's DDoS Protection

MazeBolt RADAR exceeded all the requirements defined by the customer:

Customer Requirement	MazeBolt Solution
1 Preliminary analysis, in the context of anti-DDoS tests, to identify the functionality and limits of services and tools used in the simulation of DDoS attacks	MazeBolt conducted a preliminary DDoS simulation of 10% of the customer's attack surface. This initial test identified significant vulnerabilities in all of the customer's DDoS protection layers. Based on the preliminary results, it was decided to expand the simulation to all critical services.
2 Definition and formalization of DDoS Vulnerability Management activities, to guarantee anti-DDoS tests are carried out both now and in the coming years - as per the regulations	MazeBolt methodology provides the customer with an ongoing testing and simulation service that operates continuously, with no disruption. The service runs automatically, based on an agreed plan, to ensure tests are carried out now and in the future.
3 Replication of the range of types of malicious traffic, that are perpetrated by known threat actors operating in the financial sector, such as: Killnet, NoName057(16), Anonymous Sudan, and Mysterious Team Bangladesh	MazeBolt provides coverage of over 150 DDoS attack vectors from layers 3, 4, and 7. Our research team adds new attack vectors (AVs) on a quarterly basis – based on the threats that are seen in the wild and used by known threat actors.
4 Verification of how the combination of different multi-layered defense mechanisms work together to mitigate DDoS attacks	MazeBolt's product architecture is designed to analyze hybrid, multi-layered DDoS mitigation solutions in parallel. For example, when tested against a specific AV, the result covered the vulnerability analysis of each layer: CDN, scrubbing centers, on-prem. defense, WAF, etc.
5 Development of a detailed plan for executing anti-DDoS testing activities, including a risk assessment of the execution	MazeBolt follows the Gartner CTEM framework, which includes: mapping the attack surface, testing continuously, prioritization, remediation, and validation. RADAR's continuous workflow and validation reduces the risk of partial execution.

Customer Requirement	MazeBolt Solution
6 Identifying the team and the specific individuals who are responsible for the anti-DDoS testing process (as part of the planning phase)	MazeBolt assigned a Solution Architect and Technical Account Manager who worked directly with the customer, as well as with the teams from the mitigation vendors. Together, they built a RADAR DDoS program that defined ongoing testing, remediation, and validation activities.
7 Risk mitigation measures aimed at reducing possible impacts caused by the execution of the test must be defined (as part of the planning phase)	MazeBolt's RADAR is an enterprise-grade, patented, non-disruptive DDoS testing and simulation solution. It runs DDoS simulations with no interruption to business continuity, i.e., with no maintenance windows and zero downtime.
8 Asset owners must be involved in selecting a date and time for executing the test	MazeBolt customers can run RADAR continuously. RADAR includes an automated scheduler where customers define when to run the simulations. A date and time stamp appears on all results produced by RADAR.
9 Definition of the scenarios that should be tested and the malicious traffic techniques that should be replicated	MazeBolt's knowledgebase covers all known attack vectors (over 150). The exact rate of the testing is customized after a system functional test in the customer's production environment. See: https://kb.mazebolt.com/
10 Tests must include at least: • A volumetric DDoS attack aimed at the network infrastructure • A targeted attack on the Internet Banking production perimeter	Volumetric testing of the network infrastructure can be scheduled at regular intervals, and is mainly aimed at testing the response teams (and not necessarily the protection equipment). Tests are conducted in a production environment using volumes that trigger DDoS protection mechanisms, while being non-disruptive. Test results are the only accurate way to identify all vulnerabilities across all public-facing IPs.

Customer Requirement	MazeBolt Solution
11 Development of a remediation plan, that is shared with the ICT Governance and Security Governance functions	MazeBolt's remediation report is an integral part of the RADAR solution. Vulnerabilities found in the protection solutions can be fixed and validated in every testing cycle.
12 Production of a report that contains: • All evidence regarding the identification and mitigation of cyber events • Details of the approach that was followed • Findings and observations • Advice recommending areas for improvement in terms of technological, policy and procedural controls	MazeBolt's RADAR Vendor Report is used by the customer and the mitigation vendors. It includes detailed findings of all protected and vulnerable targets, along with a detailed scope of any additional environments, targets, and systems that should be covered.
13 Drafting of a final report (executive summary) that reports the main findings of the test, to be shared with the CIO and CISO	MazeBolt's RADAR Executive Report is generated to cover the main findings, progress, and recommendations. These reports are presented to senior management and, in some cases, is shared with board members.
14 Integration of specific vulnerabilities identified during test execution into the tracking platform - and their assignment to an owner for resolution	MazeBolt RADAR includes SIEM integration via Syslog and it can send all or filtered results to the integrated system.

"MazeBolt RADAR helps us reduce the risk of DDoS attack while ensuring business continuity. MazeBolt provides us with critical DDoS insights."

-CISO, European Bank

MAZEBOLT

About MazeBolt

MazeBolt RADAR is a patented DDoS Vulnerability Management solution. Using thousands of non-disruptive DDoS attack simulations and without affecting online services, it can identify and enable the remediation of vulnerabilities in deployed DDoS defenses. RADAR enables organizations and governments to maintain the uninterrupted business continuity of online services. Using RADAR's patented vulnerability simulation technology, enterprises have unparalleled visibility into their DDoS protection solutions so they can be confident that damaging DDoS attacks can be prevented - before they happen. Read more at www.mazebolt.com