MAZEBOLT

Case Study

Leading European Bank Rebuilds DDoS Resilience

The client:
A leading multi-channel bank focused on retail banking, insurance, asset management activities, European debt capital markets, and trade finance in EU countries.
Part of the top 20 largest banks in Europe, catering to an estimated 10 million customers with nearly 45,000 employees globally in 1500 branches.
A barrage of DDoS attacks was damaging business continuity and hurting customer experience.

Key Takeaways

Challenges

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

Solution

- Implemented RADAR™

Impact

- Drastically reduced risk from 43% to under 4% (90% risk reduction).
- Continuous DDoS testing.
- Improved customer experience.

The Challenge: Increasing Visibility into DDoS Vulnerabilities

After recent DDoS attacks hampered business continuity and crippled the digital experience for customers, the bank needed to ensure the best-in-class customer experience for its 10 million customers.

The bank's CISO needed to gain visibility into the online service's infrastructure across branches, along with a holistic view of DDoS vulnerabilities before taking corrective action. Ensuring seamless digital experience and business continuity were top priorities for the bank, and DDoS protection was considered a crucial part of the overall business security strategy. Performing disruptive DDoS tests such as red team and pen testing were not viable and sufficient options for the bank.

The Solution: Eliminating DDoS Vulnerabilities with Zero Downtime

MazeBolt RADAR™ was quickly deployed in parallel to the banks' existing DDoS protection solution so that it could deliver continuous visibility of DDoS vulnerabilities across all online services.

Even when different DDoS protections services were deployed by different branches and affiliates, RADAR was able to clearly identify where the vulnerabilities were, allowing the protection vendors to quickly remediate the vulnerabilities, and re-test them to validate that the fix was performed properly.

This entire process, throughout all the branches, had no impact on ongoing operations. In addition, RADAR delivered prioritized reports across its many locations, including the bank's affiliates. Overall exposure to DDoS attacks that bypass protection layers, mostly related to layers 3, 4, and 7, as well as SSL DDoS attack vectors, was reduced from an initial vulnerability of 43% to under 4%.

The Benefit: Achieving True DDoS resilience with No Disruption to Online Services

Before deploying RADAR, the bank's applications and network displayed a 43% DDoS risk. RADAR exposed DDoS vulnerabilities on an ongoing basis to continuously optimize DDoS resilience with no disruption to online services. Customers have assured business continuity and a good customer experience. The CISO gained ongoing visibility of online services to ensure a viable security strategy, with an overall DDoS exposure reduction of 90%.

> "MazeBolt RADAR helped us to ensure business continuity, remediate vulnerabilities and retain customers even when faced with serious DDoS threats."
>
> **CISO**, leading European bank

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.