MAZEBOLT

CASE STUDY

International Bank Chooses RADAR™ to Prevent Damaging DDoS Attacks

Industry: Financial Services

Overview

A large, international bank operating in Europe and the US was facing repetitive DDoS attacks and downtime of critical online banking and third-party financial services.

The Challenge

Ongoing DDoS attacks created the following challenges:

- Unavailability of critical, customer-facing services, including online and mobile banking, and proprietary trading platforms
- Inaccessibility of third-party, connected applications (such as loan and payment apps)
- Interruption to VPN connectivity, creating issues for employees and remote branches
- Risk to open banking initiatives due to API vulnerabilities

The Solution

RADAR's nondisruptive DDoS attack simulation solution was deployed in the bank's primary data centers. RADAR identified vulnerabilities in the scrubbing center, CPE, and WAF protection layers.

First, RADAR identified the following DDoS vulnerabilities in the bank's deployed protection technologies:

- 57% DDoS vulnerability level - across layers 3, 4, and 7
- Automated DDoS protection that was only 43% effective
- DDoS protection policies that were not customized, leaving the bank exposed

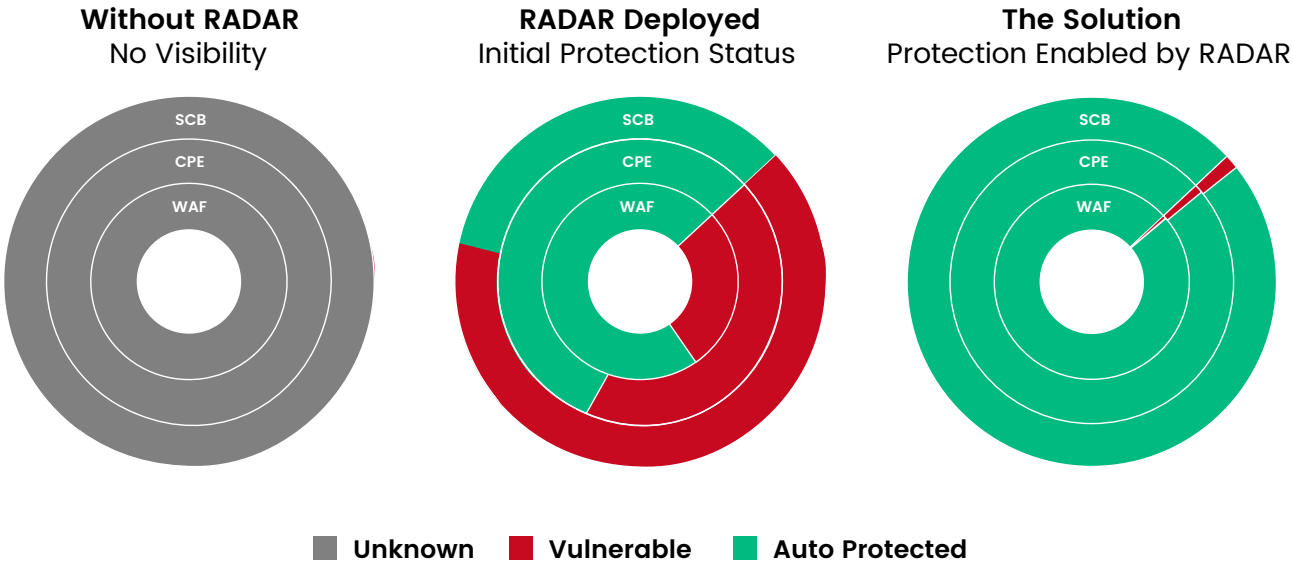
Customer Benefits

Since the bank started working with RADAR, all DDoS attacks have been mitigated automatically without any damaging downtime.

Additional benefits include:

- Improvement of automated DDoS protection by over 120% (from 43% to over 95%), enabling the bank to avoid disruption of business operations
- Reduction in cyber insurance costs
- Drop in the bank's DDoS vulnerability level - from 57% to less than 5%
- RADAR-generated reports that are key to the bank's compliance with cybersecurity regulations

Working with MazeBolt's Professional Services team, the bank was able to gain critical visibility into its DDoS protection misconfigurations and vulnerabilities - per security layer:



RADAR Identifies Vulnerabilities

Next, RADAR provided the bank with a prioritized report of identified vulnerabilities. MazeBolt's actionable remediation plan continues to be generated automatically after each cycle of RADAR attack simulations. This enables MazeBolt's team to focus on the attack vectors that present the greatest risk to the bank's environment, including: sophisticated Layer 7 attacks, Slowloris, UDP, and DNS attack vectors.

"MazeBolt RADAR helps us ensure business continuity by identifying and enabling us to remediate DDoS vulnerabilities. We gain ongoing insight into our automated DDoS protection. RADAR allows us to reliably provide online banking services to our customers, even when we are under attack."

-CISO, international 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