MAZEBOLT

RADAR™:

A Critical Breakthrough in DDoS Security

Achieve true DDoS resilience by uncovering DDoS blind spots, continuously detecting vulnerabilities and misconfigurations, analyzing traffic data, and prioritizing remediation. Maximize your DDoS protection ROI by avoiding a damaging DDoS attack. RADAR's non-disruptive, autonomous risk detection allows cybersecurity teams to solve the critical challenge of DDoS security.

The DDoS Challenge

Online services architecture has become more complex and distributed. As DDoS attacks evolve, they become more sophisticated and severe in the damage they cause enterprises. From banking to government, recent years have shown that organizations are under a false sense of security, spending millions for DDoS protection solutions that are misconfigured and cover only a fraction of their online services' security posture. Periodical red-team testing coupled with the leading DDoS protection solutions is simply not enough to have reliable DDoS resilience.

With over 23,000 DDoS attacks per day, an expected total of over 15 million DDoS attacks this year alone, and an average cost of $ 30K per hour of downtime for mid-sized organizations - damaging downtime is waiting around the corner, along with a loss of revenue, and damaged customer confidence.

Solution

RADAR is the only solution that empowers organizations to identify and eliminate all DDoS vulnerabilities – thus, taking a proactive approach to avoiding damaging DDoS attacks.

RADAR provides enterprises with full visibility into their DDoS protection through identifying and allowing for remediation of vulnerabilities on each layer of DDoS protection E.g. CDN, Scrubbing, CPE, WAF. Continuously testing tens of thousands of potential DDoS attack entry points, RADAR patented technology identifies how attackers bypass existing protection systems.

The solution's autonomous risk detection allows cybersecurity teams to adopt the new approach of preventing damaging attacks from succeeding altogether.

Continuously and non-disruptively test your online services
Visualize your entire security posture and get hard data and percentages of all known DDoS attack vectors that evade your DDoS protection layers. RADAR patented technology simulates tens of thousands of distinct attacks annually with no disruption to services.

Fully automated
RADAR is a fully automated solution that runs in the background, continuously looking for new vulnerabilities. Once scheduling is setup, it requires no operational interaction.

Identify vulnerabilities by OSI layer
RADAR checks vulnerabilities in Layer 3, 4 and 7 to protect your organization against DDoS attacks. This includes TCP, UDP, IP-Based, HTTP/S, DNS, NTP, SIP, and other attack vectors. To date, RADAR has more than 150 attack vectors.

Prioritize the most relevant vulnerabilities
Impact-based prioritization ensures DDoS protection teams resolve issues in the most effective order to close all vulnerabilities as fast as possible. With just a few fixes, dozens or hundreds of vulnerabilities may be eliminated.

Test and retest every attack vector
Schedule all DDoS attack vectors to be continuously retested or disable unneeded specific attack vectors from being tested in the future – all without interrupting business operations.

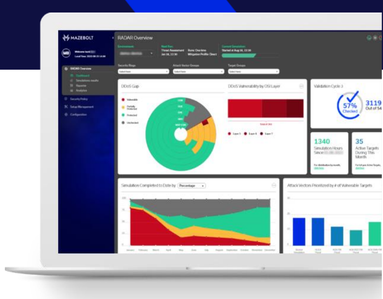
Expert support and advisors
MazeBolt's DDoS professional services and research teams are composed of experts in the fields of DDoS research and emergency response.

RADAR™

The new approach to DDoS security.

Even with the best DDoS protection solution in place, every organization suffers up to 75% exposure of their online services. RADAR's non-disruptive, autonomous risk detection allows cybersecurity teams to reinforce their existing DDoS protection systems by continuously detecting vulnerabilities and misconfiguration and prioritizing remediation.

By maintaining automated DDoS protection at over 98% with RADAR, organizations can achieve true DDoS resilience.



- Continuously test and simulate your online services and DDoS protection, with no disruption to services.
- Identify vulnerabilities by OSI Layer - 3, 4 and 7, in every protection layer: CDN, SCB, CPE, WAF.
- Test and retest over 150 attack vectors, with zero downtime.
- Prioritize your vulnerabilities with actionable insights into attack vectors, blind spots, misconfigurations, and more.
- Get Strategic Reports, Executive Reporting, ongoing consultancy, and comprehensive customer support

VISIT MAZEBOLT.COM

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. RADAR's autonomous risk detection allows cybersecurity teams to go beyond traditional DDoS testing to uncover blind spots and misconfigurations in their protection layers by continuously testing, analyzing, and prioritizing remediation with zero operational downtime. Global enterprises, including financial services, insurance, gaming and governments rely on MazeBolt for full visibility into their true DDoS security risk.