How RADAR™ Simulates DDoS Attacks and Protects Live Environments

The year 2020 observed a recorded-breaking 10 million DDoS attacks. Even now, the DDoS repercussions continue as attacks have increased in frequency and sophistication, causing maximum damage. It is relatively manageable for mitigation solutions to detect and mitigate simple threats having repetitive patterns; however, when attackers use multiple complex vectors and control the traffic flood below expected norms, mitigating threats becomes more challenging. As a result, more DDoS attacks bypass the best-of-breed mitigation systems because attackers are using new and sly tactics that mitigation systems cannot block unless configured by network-specific settings.

> The "Best Practice Setup" is Not Enough Anymore

Validate Deployed Mitigation Systems by Simulating Non-Disruptive DDoS Attacks

Organizations get blindsided by DDoS attacks because they believe that their DDoS mitigation SLA works automatically and reliably, and it fully protects their networks from DDoS threats. However, SLAs are relevant only if the deployed DDoS protection identifies the attack; if not, organizations will have to handle damaging downtime. Moreover, organizations have poor or no visibility of the DDoS vulnerability gap; therefore, they are likely to remain unprepared or taken by surprise during an actual DDoS attack. As a solution, continuously validating the effectiveness of the deployed DDoS protection is critical.

This means conducting DDoS attack simulations with a maximum number of attack vectors and intensity levels possible, including geographical diversity. DDoS attackers use a mix of different traffic patterns, threat vectors and botnets to make attacks successful and difficult to detect. Therefore, organizations are accountable for testing whether their stationed mitigation strategies can defend different modus operands and new attack tactics. This is only possible by performing ongoing, non-disruptive attack simulations on live production systems and ensuring attacks are automatically blocked in real-time when the need arises.

The Longer the Maintenance Windows, The Higher the Cost

A simulation that requires maintenance windows is costly and essentially useless because it can only validate a limited number of attack vectors & targets at a single time. For example, a typical small network has around 5000 potential entry points for attackers, and only around 20 can be identified during such a single maintenance period. That is just 0.4% of all entry points. As a result, disruptive DDoS attack simulations are not valid in assessing the effectiveness of DDoS protection levels.

RADAR™ Technology - DDoS Simulator on Live Environments

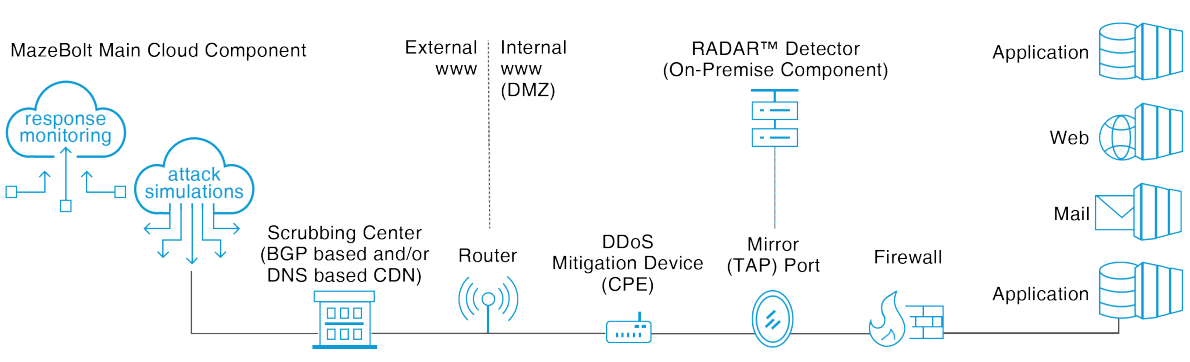
RADAR™, MazeBolt's transformative and patented technology, is the only 24/7 automatic DDoS attack simulator on live environments with ZERO disruption/downtime. Compatible with all mitigation solutions, the technology automatically detects, analyzes, and prioritizes the remediation of DDoS vulnerabilities across the network. As a result, mitigation solutions can effectively prevent all DDoS attacks only when deployed with RADAR™.

RADAR™ Works on Two Key Components:

1. The Cloud Component simulates incremental DDoS attack vector traffic (starting at a low rate and increasing as required). It has response monitoring capabilities that create normal baseline response times for services in production. The Cloud Component identifies new potential targets that are susceptible to attacks from external threat actors.

2. The On-Premise Component (RADAR™ Detector) monitors all simulated traffic downstream from the DDoS mitigation device or scrubbing center on a mirror port during a simulation. The On-Premise Component detects attack leakage for immediate remediation.

The DDoS RADAR™ Network Setup



RADAR™ Simulation Without Disruption Operates as Follows:

1. Before launching any attack simulation, RADAR™ establishes an understanding of "Response Monitoring Baselines" i.e. how long it takes for the target systems to answer requests; this is done from multiple locations around the world. All selected services and targets have response monitoring applied automatically, and response baselines are recorded and maintained.

2. The Cloud Component automatically probes different ports at all IP addresses that help the clients in understanding their security posture.

3. A specific attack vector is simulated so that the target DDoS mitigation can detect and block it. During the simulation, the following occurs:
   - RADAR™ records the “Response Monitoring Baselines” from the target across multiple locations, ensuring no impact occurs to the targeted service.
   - DDoS attack simulation is gradually increased to the automatically adjusted rate for the specific target and monitored throughout the simulation.
   - If RADAR™ detects any deviation in monitoring baselines i.e. from the normal response times, the cut-off mechanism is activated and simulations are automatically and immediately stopped. A deviation refers to an increase in response time between 5 and 50 milliseconds.

4. The On-Premise Component (RADAR™ Detector) continuously checks if any leakage has occurred during the attack simulations.

5. The status of the target network is then calculated as protected or vulnerable based upon the detected attack leakage.

6. Additional pre-attack simulation checks are performed, with different layers of cut-off mechanisms ingrained into the RADAR™ technology and operated system-wide all the time.

How RADAR™ Protects Live Environments

RADAR™ simulates a "Full DDoS Attack", where each attack simulation is preset to trigger the deployed DDoS security systems that detect and block all DDoS attacks. The security systems are configured to get triggered when such a specific DDoS attack is being simulated. Therefore, during an attack simulation, if the security systems do not get triggered; it means the systems will fail to mitigate the real DDoS attack vector automatically, causing damaging downtime.

RADAR™ does not intentionally cause deviations to mark off the target as vulnerable. The attack simulations evaluate how the network is protected to block a real DDoS attack and if the deployed mitigation can successfully avoid the DDoS downtime.

Almost all downtime caused by a DDoS attack occurs because network vulnerabilities remain undetected, in addition, the best available DDoS protections deployed are not adapted to the specific environment, and the security mechanisms are not triggered when required, i.e., at the time of a real DDoS attack.

As part of digital transformation, organizations continually update their production environments, making them more vulnerable to DDoS attacks. RADAR™ validates the impact of these network changes upon the deployed DDoS mitigation solutions and detects over 9000 vulnerabilities a month on specific production systems. As a result, organizations can have real-time information about their DDoS vulnerabilities and can be more prepared than ever.

RADAR™ prioritizes network vulnerabilities for immediate remediation and validates them without any disruption or manual intervention. Deploying a DDoS simulator on live environments that maximizes the efficiency and reliability of the deployed mitigation solution is the key to blocking all DDoS attacks. As the technology wasn't available earlier, organizations couldn't think of identifying real-time DDoS vulnerabilities without causing disruptions.

However, by deploying RADAR™, organizations can now fully protect their live environments from DDoS attacks and avoid any complex response scenarios or emergencies.

Request a Demo

More about RADAR™