

DDoS attacks continue to increase in frequency and sophistication, causing maximum damage. More DDoS attacks bypass deployed mitigation systems because attackers are using new tactics and complex attack vectors that mitigation systems cannot block unless configured by network-specific settings. The "best practice setup" is not enough anymore to stop all DDoS attacks.

Organizations have poor or no visibility of their DDoS Protection effectiveness in "peace-time". Therefore, they are likely to remain unprepared or taken by surprise during an actual DDoS event. The growing DDoS mayhem is an alarm for organizations to **prioritize and validate their DDoS Protection**.

Simulating DDoS Attacks is a crucial necessity to visualize and react to vulnerabilities identified in your deployed DDoS protection, which helps maintain business continuity. Performing ongoing, non-disruptive attack simulations against production systems is the only way to assess your DDoS protection level in peace-time and ensure that it can **automatically block attacks in real-time** when the need arises.

Maintenance Windows on Production Do More Harm than Good

The longer the maintenance windows, the higher the cost. Additionally, simulations **which require disruption** are very limited by nature in deciding how many attack vectors & targets can be validated. A typical small network has around 5000 potential entry points for attackers, and maybe 20 can be checked during such a maintenance period, that's just **0.4%**.

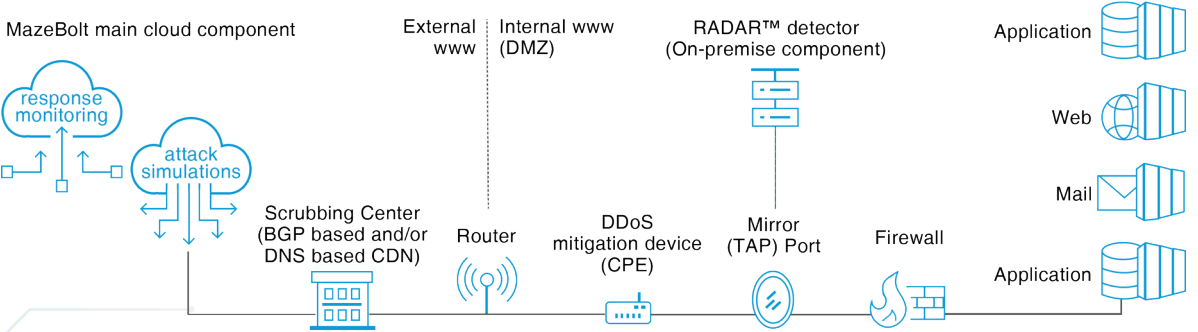
Disruptive DDoS attack simulations are **essentially useless** in assessing DDoS vulnerability levels.

RADAR™ - DDoS Simulation on Live Environments

The RADAR™ patented technology works on two key components:

- 1) **A Cloud Component** – a) Simulates incremental DDoS attack vector traffic (starting at a low rate and increasing as required). b) Has response monitoring capabilities which creates normal baseline response times for services in production. c) Additionally, the cloud component identifies new potential targets that are susceptible to attack from external threat actors.
- 2) **An 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 RADAR™ detector **detects attack leakage**.

The DDoS RADAR Network Setup



A Typical RADAR™ simulation without downtime operates as follows:

- 1) The cloud component automatically probes different ports at all IP addresses and understands the client's security posture.
- 2) All identified services and targets automatically have response monitoring applied, and response baselines are created and maintained.
- 3) A specific attack vector is simulated so that the target DDoS mitigation can **detect and block it**. During the simulation, the following occurs:
 - a) Response monitoring is checked (against the target being simulated) from multiple continents, ensuring no impact is occurring to the targeted service whose security is being validated.
 - b) DDoS attack simulation is increased to the automatically adjusted rate for the specific target and profile.
 - c) **Cut-off mechanism - If any deviation** (in milliseconds) from normal response times is detected, simulations are automatically and immediately stopped.
- 4) The on-premises component (RADAR™ detector) continuously checks if any leakage has occurred during attack simulations.
- 5) Based upon attack leakage detected, the status of **protected** or **vulnerable** is calculated.

To Prevent Disruption, before launching any attack simulation, RADAR™ patented technology establishes an understanding of how long it takes for your systems to answer requests; this is done from multiple locations around the world; we call these "Response Monitoring Baselines". Then, when a DDoS simulation is running, RADAR™ increases the monitoring speed, and if it detects a deviation in monitoring baselines, the attack simulation traffic is immediately stopped. A "deviation" refers to an increase in response time between 5 and 50 milliseconds. 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.

NOTE

It is important to note that RADAR™ is **primarily concerned with attack simulation leakage** to determine if a target is protected or vulnerable. RADAR™ does not intentionally try to cause deviations to come to conclusions about potential vulnerability statuses.

- RADAR™ simulates a "Full DDoS Attack", where each attack simulation is designed to **trigger DDoS security mechanisms (detection & blocking)**. These security mechanisms are configured to get triggered when such specific type of DDoS attack is being simulated. However, suppose the security mechanisms are not triggered during an attack simulation. In that case, it means a real DDoS attack will **not be mitigated automatically** when an attacker uses such a DDoS attack vector, causing damaging **downtime**.
- Almost **all downtime caused by a DDoS attack** occur because the best available DDoS protections deployed are not adapted to the specific environment (leaving many in place vulnerabilities), and the security mechanisms **are not triggered when required, i.e at the time of the real attack**.
- RADAR™ can detect over 9000 vulnerabilities a month on specific production systems, all **without any disruption or manual intervention**.
- As part of digital transformation, organizations continually update their production environments, making them more vulnerable. RADAR™ validates the impact of these network changes upon the deployed DDoS mitigation solution/s.
- Because RADAR™ requires no disruption to production services, **remediation and immediate validation** of fixes to prioritized vulnerabilities is made possible. This practically transforms the automated abilities and the **reliability of DDoS protections deployed**, essentially eliminating the likelihood of any succeeding DDoS attack.

Request a Demo



RADAR™, MazeBolt's transformative technology, is the only 24/7 automatic DDoS attack simulator on live environments with ZERO downtime/disruption. Mitigation solutions are more effective when deployed with RADAR™. Compatible with all mitigation solutions, RADAR™ automatically detects, analyzes, and prioritizes the remediation of DDoS vulnerabilities across the network.

More about RADAR™ on Our Website



By adding RADAR™, organizations can monitor and close vulnerabilities continuously and dramatically increase their deployed mitigation solution's efficiency by blocking all DDoS attacks.