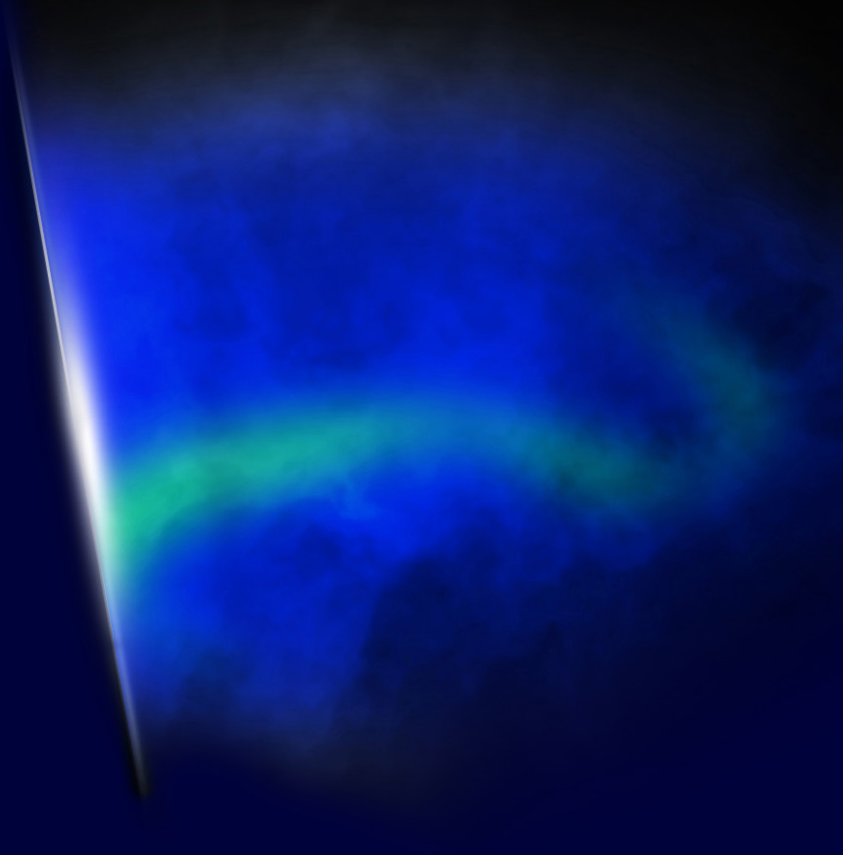
MAZEBOLT

Maximize DDoS resiliency with continuous RADAR™ testing



Key Benefits

- **Continuous and frictionless** detection of DDoS vulnerabilities
- **No maintenance** window required
- Covering all public-facing **IPs and FQDNs**
- **Quickly validates** remediation of configurations
- **Seamlessly works** with all the organizations' mitigation layers
- Maintain business as usual with **zero downtime**

Components

Cloud

Validates DDoS vulnerability level by transmitting a controlled DDoS attack to the monitored target.

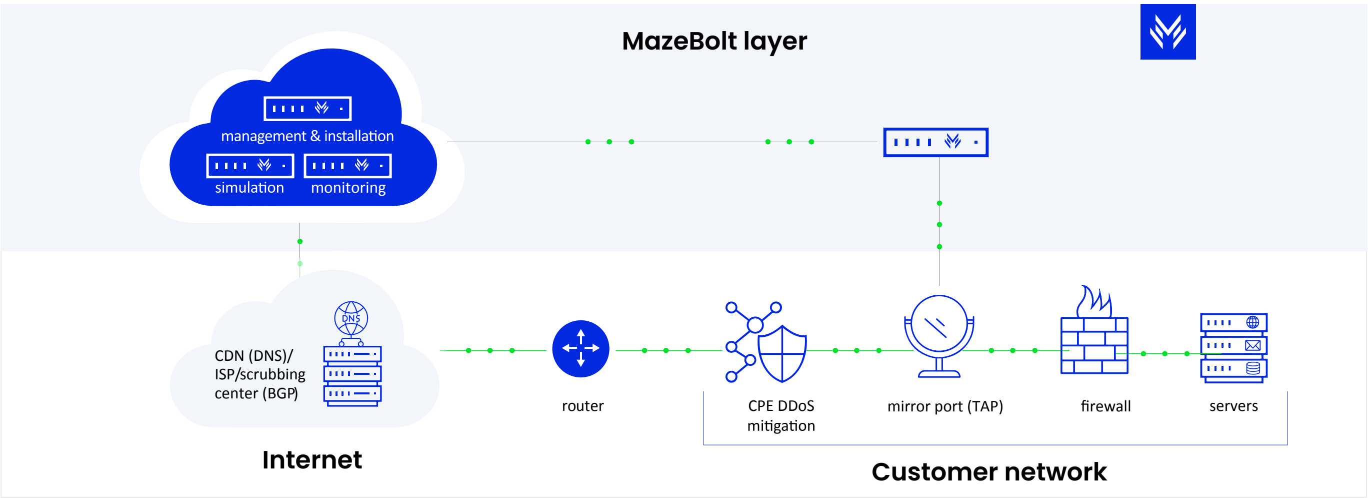
Identifies real-time changes in response times during validation.

Monitors the target's response time by sending legitimate requests to the targets and measuring the time taken to get a response.

On-Premise

Sychronizes with cloud component before and after each test.

Monitors all traffic downstream from the DDoS mitigation device or scrubbing service during the test to identify leakage.



Network Setup Technical Specifications

Deployment Considerations

RADAR™ testing currently validates the supported setups listed below:

- Datacenter with CPE equipment protection
- Datacenter with BGP scrubbing center service protection
- Datacenter with a hybrid of CPE and scrubbing center protection
- GCP (Google Cloud) & AWS (Amazon Cloud)

Other Deployment Considerations

- Deploy immediately after DDoS mitigation
- Connection to MazeBolt's API via management port
- Ability to read true source IPs

Security Considerations

MazeBolt's platform and RADAR™ testing adhere to strict security standards:

- Secure coding practices and ISO 27001 compliant
- Fully installed and quality assured hardware
- All intercommunication to and from the DDoS RADAR™ testing, incoming and outgoing, is encrypted using TLS (HTTPS). No private data (PII) is captured, used, or exposed
- MazeBolt's platform is secured using TLS (HTTPS) and two-factor authentication

Over
50,000
vulnerability attack simulations annually

140+
simulations against each target

98%
automated protection

100%
uptime and attack surface coverage

MazeBolt is pioneering a new standard in testing DDoS mitigation that provides enterprises with full attack surface coverage. Its vulnerability solution, RADAR™ testing, continuously observes tens of thousands of potential DDoS attack entry points, identifying how attackers succeed in bypassing existing mitigation systems. The solution's autonomous risk detection allows cybersecurity teams to go beyond traditional DDoS testing by continuously detecting, analyzing and prioritizing remediation across the network with zero operational downtime. Global enterprises, including financial services, insurance, and governments rely on MazeBolt for full visibility and complete DDoS protection. **For more information visit www.mazebolt.com.**

MAZEBOLT