MAZEBOLT DATASHEET

Continuous Detection and Elimination of DDoS Threats

Distributed denial-of-service (DDoS) attacks are increasing in scale and ferocity, overwhelming businesses globally. The number of DDoS attacks doubled in the first quarter of 2020 compared to Q4 2019 and 80% more than in Q1 2019. The attacks are launched with stealth using high volume traffic and low and slow application targeting. Professional hackers are constantly seeking new ways to disrupt traffic flow, discolor customer experience and inevitably lead to loss of revenue.

RADAR™, MazeBolt's new patented technology, provides a top layer to any DDoS mitigation system providing continuous DDoS threat simulations without any disruption or need for maintenance windows. It assists organizations in achieving, maintaining, and verifying the continuous closing of their DDoS vulnerability gaps. Reducing and maintaining the vulnerability level from an average of 48% to under 2%.

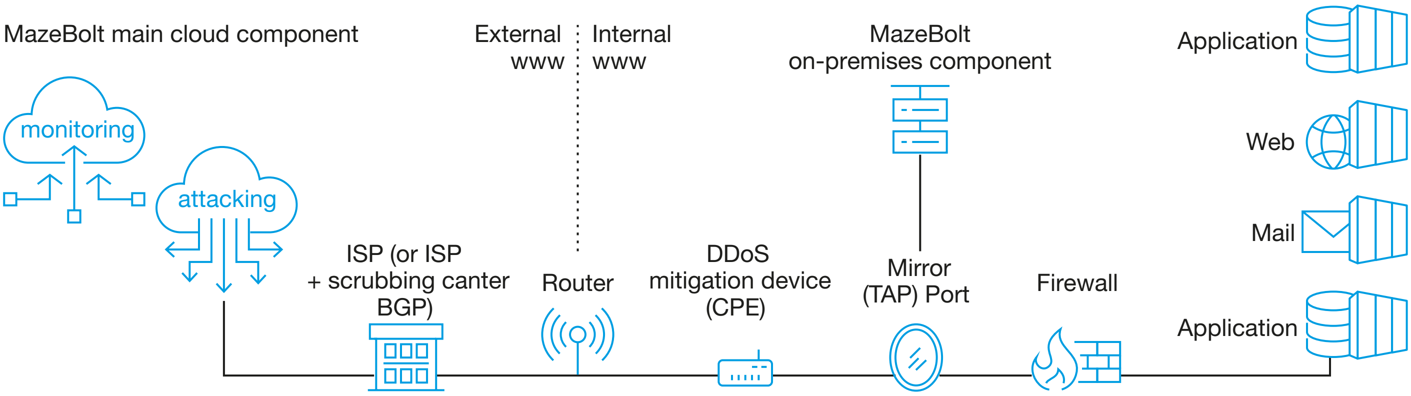
What's Inside?

- Eliminate DDoS vulnerabilities to under 2%
- Continuous and automated non-disruptive detection of DDoS vulnerabilities
- No maintenance windows required
- Covering all IP ranges. 100+ simulations against each IP
- More than 50,000 vulnerability attack simulations annually
- Quickly validate remediation of configurations
- Managed service - Professional services to guide remediation identified vulnerabilities
- RADAR™ works with any mitigation platform to provide end to end full coverage

The DDoS RADAR™ Components

Cloud Component	On-Premise Component
1 // Monitors the target's response time by sending legitimate requests to the targets and measure the time taken to get a response 2 // Validates DDoS vulnerability level by transmitting very low rate DDoS attack to the monitored target 3 // Identifies real-time changes in response times during validation	1 // Synchronizes with cloud component before & after each test 2 // Monitors all traffic downstream from the DDoS mitigation device or scrubbing service during test to identify leakage

The DDoS RADAR™ Network Setup


MazeBolt main cloud component
monitoring
attacking
External www
Internal www
MazeBolt on-premises component
ISP (or ISP + scrubbing canter BGP)
Router
DDoS mitigation device (CPE)
Mirror (TAP) Port
Firewall
Application
Web
Mail
Application

Technical Specifications

Deployment Considerations	Security Considerations
The DDoS RADAR ™ currently validates the supported setups listed below: • Datacenter with CPE equipment protection • Datacenter with BGP scrubbing center service protection • Datacenter with a hybrid of BGP and scrubbing center protection Other Deployment Considerations: • Deploy after DDoS mitigation • Able to read true source IPs • Management Port • Services Scanning • DDoS RADAR™ simulation	MazeBolt's platform and DDoS RADAR™ adheres to strict security standards: • Secure coding practices and ISO compliant • Fully installed and quality assured hardware along with virtual platforms • All intercommunication to traffic from the DDoS RADAR™, incoming and outgoing, is encrypted using TLs (HTPS) • No private data is captured, used or exposed. • MazeBolt's platform is secured using TLS (HTTPS)

Why DDoS RADAR™

Description	Red Team DDoS Testing	Mitigation	MazeBolt RADAR™
Downtime under successful attack	YES	65%	NO
Testing frequency	About twice a year	N/A	Continuous
DDoS attack vectors checked per target	Less than 20	N/A	More than 100
How many target IP's tested - Against all attack vectors	Sample - Under 5 IP's	N/A	Complete - Over 1000 IP's
Vulnerability gap	48%	48%	Under 2%
Vulnerability reports	Per test	NO	Continuous - Daily
Cost	$	$$$	$$
Attack response	N/A	Reactive when an attack happens	Continuous before an attack happens
Detection of successful attacks	Sample only at time of test	During attack	Full detection - Before an attack & continuous
Added costs for Red Team testing - On Demand	YES	YES	NO

About MazeBolt

MazeBolt is a leading innovative cyber security company, and part of the mitigation space. Offering full DDoS risk detection and elimination. Working with any mitigation system to provide end to end full coverage. Avoiding downtime and eliminating mitigation vulnerabilities before an attack happens.

For more information,
please visit: www.mazebolt.com
or e-mail: info@mazebolt.com