MAZEBOLT

3 New Approaches to DDoS Vulnerability Management

Based on the DDoS Handbook for CISOs and Security Leaders

It's Proactive

1

Identify and enable the elimination of DDoS vulnerabilities ahead of time, without disruption to business continuity.

MazeBolt RADAR™ Dashboard



It's Continuous

2

Perform automated, continuous DDoS simulations on live, production services.



It's Comprehensive

3

Validate targets and services, across the DDoS attack surface, against all known vulnerabilities.



Why Now?

A dramatic **200% rise** in DDoS attacks emphasizes the escalating cyber threat landscape.

Source: Zayo Report

Limitations of Traditional DDoS Testing

Timing

Typically occurs once a year, as disruptive maintenance windows are required

Scope

Covers a restricted number of DDoS attack vectors (typically less than 2%)

Cost

Testing can lead to staffing, productivity, and revenue losses due to downtime

Read the DDoS Handbook for CISOs and Security Leaders

Download the eBook

MAZEBOLT