

# 3 New Approaches to DDoS Vu nera bility **Nanagement**

Based on the DDoS Handbook for CISOs and Security Leaders

#### It's Proactive

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

Threat Assessment | Runs: One time

Attack Vector Groups

Oct 23, 22:30

Mitigation Profile: Direct

MazeBolt RADAR™ Dashboard

**RADAR** Overview

Demo Device

Security Rings

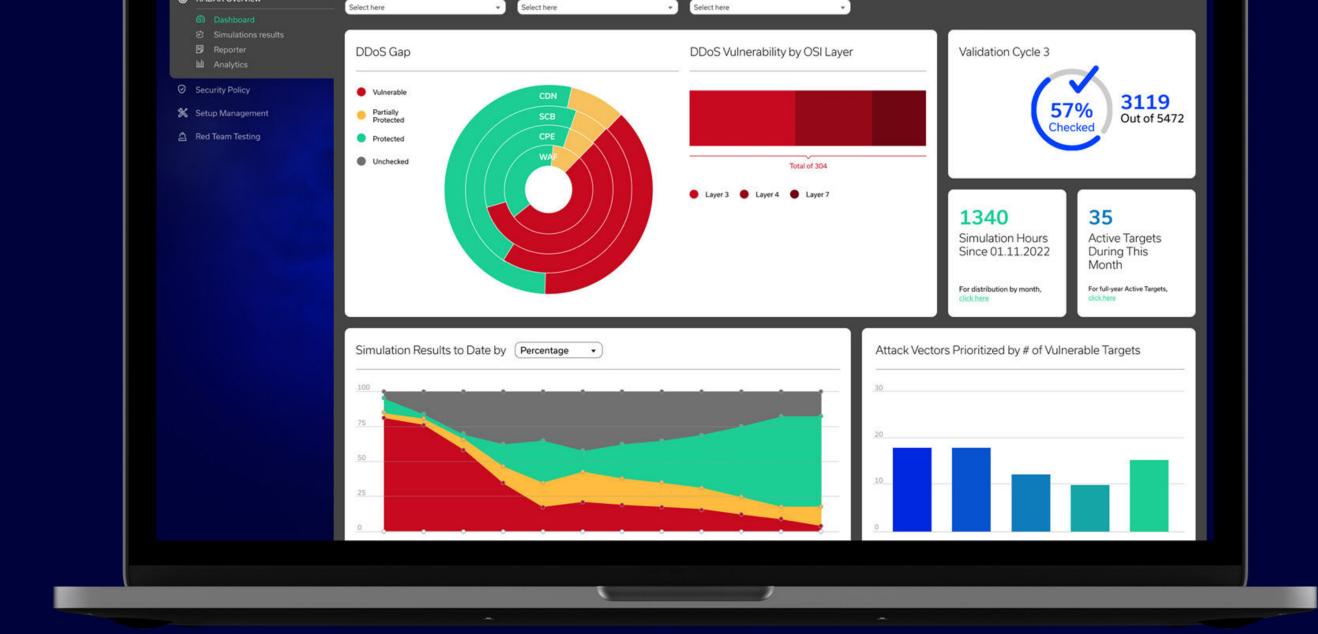
MAZEBOLT

(b) RADAR Overview

(US)

Welcome back User!

Local Time: 2023-10-22 13:30



Started at Oct 21, 22:30

**Target Groups** 

### It's Continuous

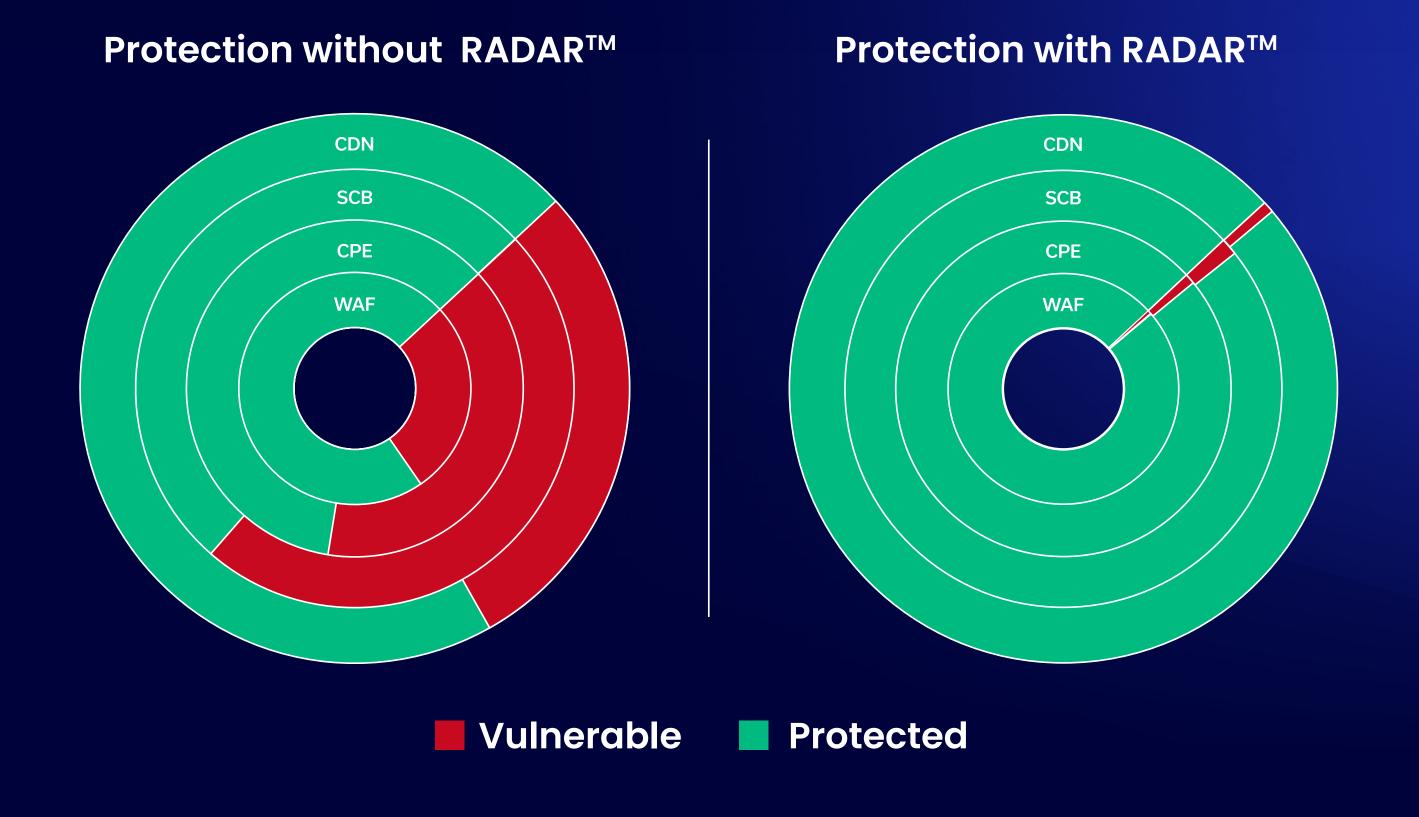
Perform automated, continuous DDoS simulations on live, production services.

scope Diagnosis Action oiscover NOOIII

## It's Comprehensive

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 tor **CISOs** and Security Leaders

Download the eBook

