MAZEBOLT

MazeBolt RADAR™

Test, Remediate and Validate Your DDoS Protections

RADAR™ is a critical component of security control testing, as it ensures the resilience of any DDoS protection solution against cyber threats across the entire attack surface. With automated and nondisruptive DDoS simulations, organizations can:

- Evaluate the effectiveness of their mitigation strategies
- Identify potential vulneraiblities in the network and application infrastructure
- Validate performance of third-party protection services

KEY BENEFITS:

- Avoid damaging downtime
- Optimize investments in DDoS protection
- Proactively enhance automated protection
- Meet regulatory requirements
- Prioritize remediation of the attacks most likely to cause damage

RADAR's patented technology transforms the DDoS Protection market by identifying vulnerabilities prior to an attack and enabling their elimination. RADAR continuously runs thousands of attack simulations scrutinizing every possible vulnerability – with zero disruption to online services.

RADAR's SmartCycle™ feature provides AI-powered prioritization of DDoS vulnerabilities. SmartCycle makes DDoS vulnerability validation a realistic possibility, even for enterprises faced with extensive attack surfaces spanning millions of potential attack points.

Gartner Peer Insights™

"The product is reliable and simulates an attack without actually damaging the site."
5.0 ★★★★★ 100%

"I have been working with MazeBolt for 2 years and my experience is excellent."
5.0 ★★★★★ 100%

"We achieve robust site security with MazeBolt's innovative simulations."
5.0 ★★★★★ 100%

"Flexible, strong product."
5.0 ★★★★★ 100%

MAZEBOLT

Test and Validate DDoS Protections on Live Production Services

For enterprises with critical, always-online services, RADAR is the only continuous DDoS Vulnerability Management solution that runs on live production services.

RADAR identifies misconfiguraitons (vulnerabilities) in DDoS protections that can be exploited to cause damaging downtime. With RADAR, you can:

MAP

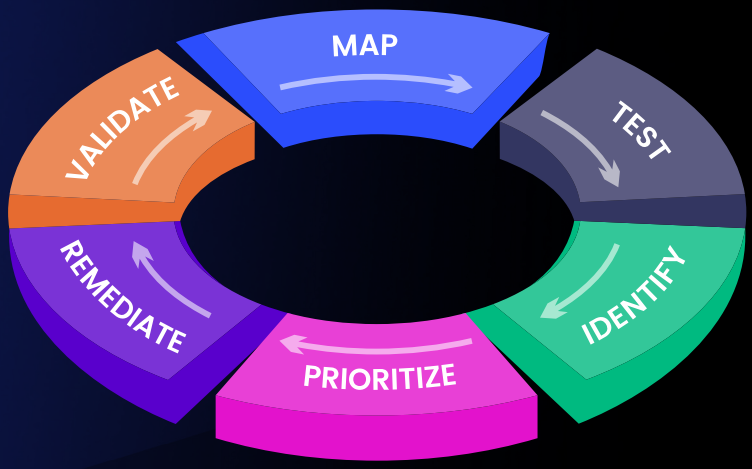
Map all public-facing services (IPs and FQDNs)

VALIDATE

Ensure vulnerabilities are patched and do not return

TEST

Continuously test all layers of DDoS protection solutions



REMEDIATE

Create prioritized remediation recommendations

IDENTIFY

Uncover DDoS vulnerabilities

PRIORITIZE

Determine which misconfigurations pose the greatest risk

Valued Partners

F5 · Microsoft · AVORD · bip. · TCSS Trusted Cyber Security Solutions · pylones* · longwave ZUCCHETTI · CNS Outsourcing IT · PAND-NET · Forcerta · G Data

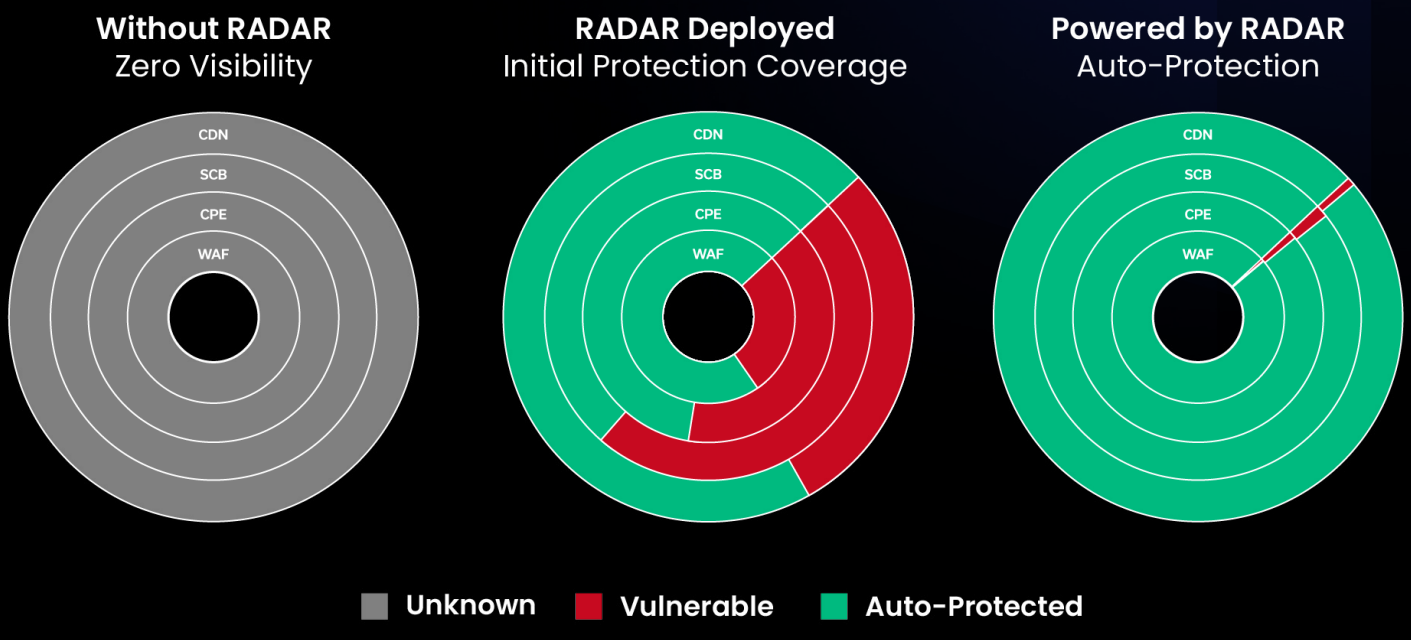
MAZEBOLT

The Hidden Gaps in DDoS Defenses

Traditional approaches to DDoS defense do not stop damaging downtime. That's because:

- **SLA guarantees are triggered only after an attack causes damage** – Even the solutions with always-on, "automated" protection or high-capacity DDoS protections are regularly bypassed by DDoS attacks. SLAs are used to remediate and recover, but the damage is already done.
- **Networks evolve over time** – DDoS protections are not built to adapt to the changes that occur over time. Even simple attacks succeed because defenses get outdated. DDoS vulnerabilities creep in, and the protections fail.
- **Red Team testing covers less than 1%** - Traditional Red Team testing checks only a small fraction of the DDoS attack surface, leaving enterprises highly exposed.

To avoid damaging DDoS attacks, you must continuously identify and eliminate the critical vulnerabilities in your DDoS protection solutions:



RADAR Closes DDoS Protection Gaps

MAZEBOLT

About MazeBolt

MazeBolt RADAR™ is a patented solution addressing the highly vulnerable DDoS protection market. Without affecting online services, through ongoing nondisruptive DDoS attack simulations, RADAR continuously identifies and enables remediation of DDoS vulnerabilities that lead to damaging downtime. Global enterprises trust RADAR to proactively prevent damaging attacks, eliminating reliance on reactive manual responses or SLA guarantees. With its unique technology, RADAR provides unparalleled visibility into defense configurations, empowering organizations to prevent attacks entirely and maintain uninterrupted business continuity. Learn more at www.mazebolt.com.