MAZEBOLT

DDoS Vulnerability Management

Protecting Your Organization from DDoS Attacks



How are DDoS Vulnerabilities Mitigated?

Patching a DDoS vulnerability in the protected device or service may require multiple adjustments:

- Changing configurations
- Applying new policies
- Enabling different measures or mechanisms
- Changing rate values

Understanding DDoS Attacks

The best way to minimize DDoS vulnerabilities involves:

TEST	Continuously test all layers of DDoS protection solutions
IDENTIFY	Uncover DDoS vulnerabilities
REMEDIATE	Create prioritized remediation recommendations
VALIDATE	Ensure vulnerabilities are patched and do not return

DDoS security differs from other types of cybersecurity in several important ways:

1. DDoS security relies on automated DDoS protection to avoid damaging DDoS attacks.
2. The only reason a DDoS attack succeeds is when the automated DDoS protection solution has a vulnerability.
3. Vulnerabilities typically arise from misconfigurations of DDoS protection security policies.
4. DDoS vulnerabilities exist in the DDoS protection policies, unlike CVEs or proprietary software bugs.
5. Mapping each DDoS vulnerability to each security layer and solution allows for efficient remediation.

Impact of DDoS Vulnerability Management

DDoS Protection without Vulnerability Management



DDoS Protection with Vulnerability Management



Protected if attacked:
Automatically blocked = no downtime

Vulnerable if attacked:
Manual intervention required = damaging downtim

Interested in learning more about DDoS Vulnerability Management?

BOOK A DEMO



MAZEBOLT