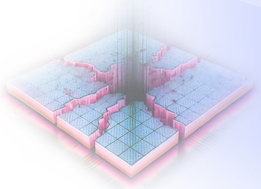
MAZEBOLT

Inside a DDoS Attack: Mapping the Hidden Gaps



A DDoS vulnerability is a combination of the following:

{DDoS Attack Vector + Target (IP or FQDN) + Service Port}

The following is one example:

SYN Flood + example.com + 443

DDoS Protection Is Layered – So Are the Gaps

Identify in which layer the DDoS vulnerability resides. For example:

SYN Flood + example.com + 443

Scrubbing=Vulnerable | On-premises=Protected | WAF=Protected

In this case, the SYN Flood attack wasn't stopped at the Scrubbing Center – but it was blocked by the on-prem. firewall and WAF.

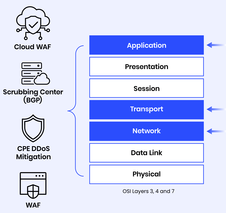
- ✕ Scrubbing Center
- ✓ On-prem. Firewall
- ✓ WAF

Close the Holes that Attackers Love to Exploit

Patching a vulnerability in the DDoS protection solution may require multiple adjustments, including:

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

Identify DDoS Vulnerabilities in All Defense Layers



Continuous DDoS Testing is the Only Way to Stay Ahead

1. **Map** public-facing services
2. **Test** DDoS protections
3. **Identify** known DDoS vulnerabilities in all defense layers
4. **Prioritize** highest risk vulnerabilities
5. **Remediate** these vulnerabilities
6. **Validate** vulnerabilities have been fixed

Want the full breakdown?

Download the eBook

MAZEBOLT