MAZEBOLT

Anatomy of a DDoS Attack

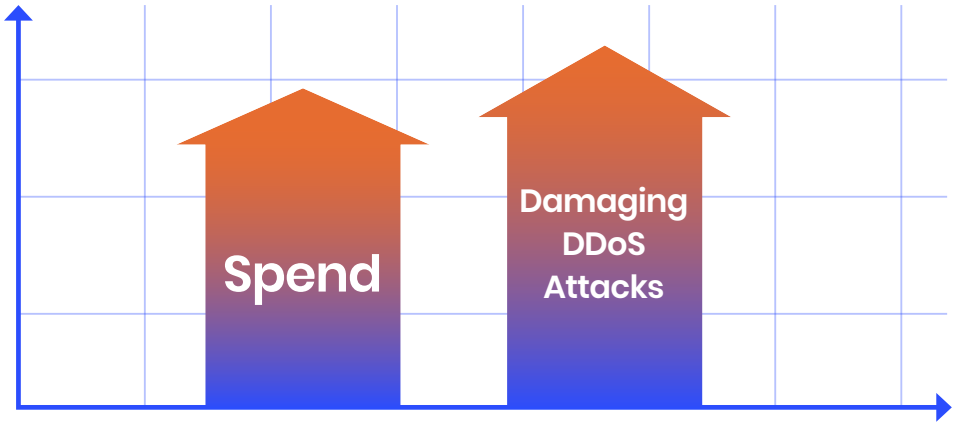
Understanding the Hidden Gaps in DDoS Protection

Table of Contents

Executive Summary	3
Even Simple Attacks Bring Down the Best DDoS Protections	3
DDoS Vulnerabilities vs. Other Types of Vulnerabilities	4
The Unknown Threat in Your Cyber Defenses	5
How DDoS Protections Get Exposed	6
Closing Holes that Attackers Love to Exploit	7
The DDoS Reality Check	9
Eliminate the DDoS Protection Gap	10
About MazeBolt	11

Executive Summary

Despite the widespread adoption of DDoS protection solutions, disruptive DDoS attacks continue to make headlines. Organizations invest increasing sums in the best DDoS protection solutions but continue to be brought down. Why? Even "basic" attacks are bypassing established defenses, as evidenced by the recurring DDoS attacks on well-known companies like X.



Companies Spend More but Still Suffer Damanging DDoS Attacks

Our analysis, based on over 100,000 hours of annual attack simulations, reveals that all deployed DDoS protections are highly vulnerable — with gaps that often go unnoticed until an attack successfully disrupts services. With no effective way to address these weaknesses preemptively, organizations remain exposed.

This eBook examines why DDoS attacks persist and continue to cause significant damage.

Even Simple Attacks Bring Down the Best DDoS Protections

More than 25 million damaging DDoS attacks were reported this year - representing a 53% YoY increase. Moreover, the volume and magnitude of these attacks increased by 56%. The total Web DDoS attacks surged 550%. These growing numbers and their escalating cost begs the question: What are we missing? And how can the risk of these attacks - and the damage they cause - be reduced?

Unlike other types of cyberattacks, the only way a DDoS attack can succeed in damaging online service availability is by exploiting vulnerabilities in the deployed DDoS protections.

In other words, the only way you can have a damaging DDoS attack (once you have protections deployed) is due to DDoS vulnerabilities in DDoS protection security policies. Cloudflare, Akamai, AWS Advanced Shield, etc. don't go down when a damaging attack occurs. It's the end customer's organization that does.

DDoS Vulnerabilities vs. Other Types of Vulnerabilities

To illustrate the importance of eliminating DDoS vulnerabilities, let's evaluate how DDoS vulnerabilities compare to other types of vulnerabilities.

Take, for example, the case of vulnerabilities in web applications: From a theoretical perspective, there would be no need to deploy a Web Application Firewall (WAF) if your Web application were to be continuously validated pre- and post-deployment, and if you followed an ongoing process of checking for vulnerabilities that included:

Static/dynamic application security testing

Manual penetration testing

Secure Software Development Life Cycle (SDLC)

Vulnerability scanning

Patch management

If this process were to be followed carefully – there would be zero errors in the coding (CVEs/proprietary) or in the logic of the web application that could be exploited. WAF would be completely unnecessary.

But this logic does not apply to DDoS vulnerabilities . The only possible protection against a DDoS attack is provided via DDoS mitigation solutions. Unlike WAF - in the case of DDoS vulnerabilities, there is no software engineering (on the end service) that could help you prevent an attack from taking down your online services.

> **When it comes to DDoS, organizations are reliant on fully automated DDoS protection solutions for damage prevention.**

If the DDoS protection solution your organization is using fails because it had a vulnerable setting – the DDoS attack causes damage and brings down services.

The Unknown Threat in Your Cyber Defenses

DDoS vulnerabilities are hidden within all DDoS protection solutions – i.e., they are mostly located in the security policies that have become outdated due to the continuous changes in network configurations, and organizations have no visibility into them. An organization can suffer a damaging DDoS attack only if its DDoS protection is vulnerable.

A DDoS vulnerability is defined as a combination of the following:

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

The following is one example of a potential DDoS vulnerability:

SYN Flood + example.com + 443

If an attacker launched the above combination against the target example.com:

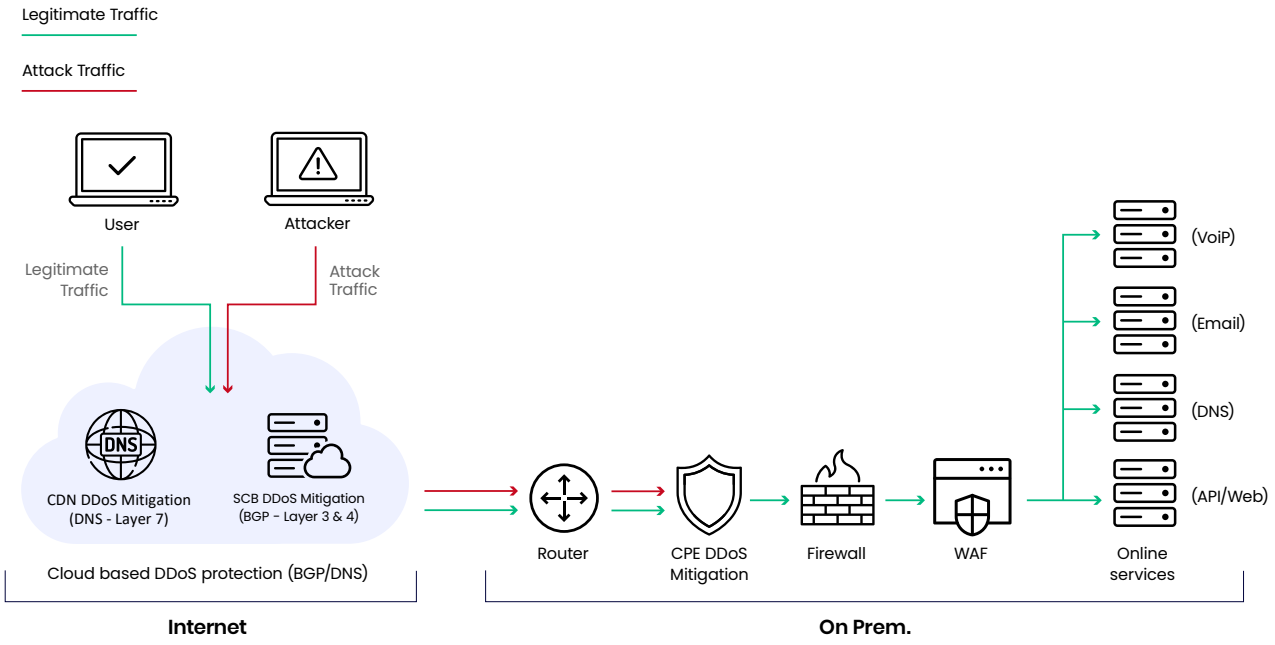
- The target is classified as protected from the particular attack vector and service combination, if the target's protection solution automatically blocks the attack (the SYN flood).
- The target is classified as vulnerable to the particular attack vector and service combination, if the target's protection solution does NOT automatically block the attack (the SYN flood), in which case manual intervention would be required - i.e., SLAs are required during a damaging DDoS attack, to mitigate manually.

Stated differently, the results of the attack will be one of these two options:

Protected	Vulnerable
The attack is automatically mitigated by protections	The attack is NOT automatically mitigated by protections
The potential vulnerability is already patched	Requires emergency response
There is no damaging downtime	Vendor SLAs are triggered
	Time to mitigation is unknown
	Patching is always post-damage

How DDoS Protections Get Exposed

Effective DDoS protection requires multiple (hybrid) layers of protection. Associating a DDoS vulnerability with the relevant protection layer is critical for successful remediation as vulnerabilities can only be remediated in the relevant protection policy.



Topology of DDOS Protection Layers

Where there is just a single layer of protection, e.g., the Scrubbing Center, it is obvious where the vulnerability is located – it will be in the Scrubbing Center itself. However, many organizations have on-prem. data centers and cloud deployments, and all are governed by multiple DDoS security layers: Scrubbing Center, WAF, cloud WAF, etc. If there is more than one layer of DDoS protection, it is important to identify in which layer the DDoS vulnerability resides. For example:

SYN Flood + example.com + 443

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

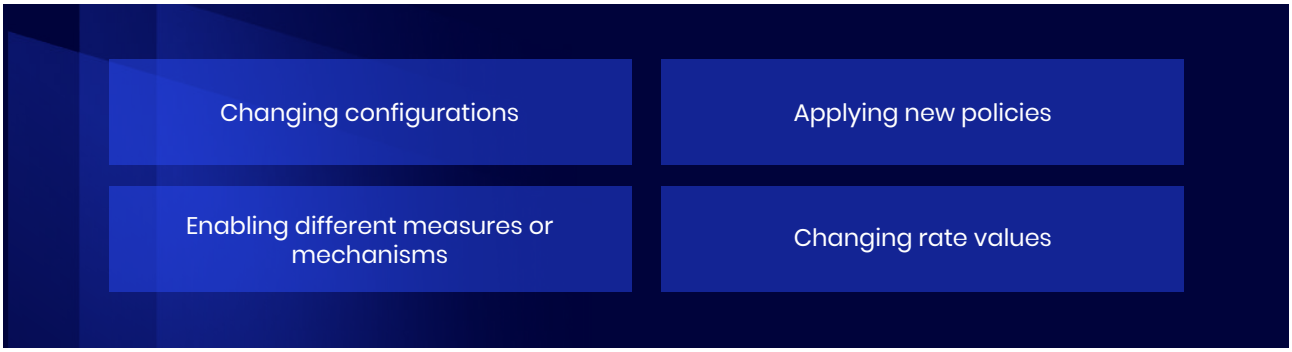
In this example, the SYN flood penetrated the vulnerability in the Scrubbing Center security policy, but the on-prem. devices and WAF mitigated it. This information allows decision-makers to decide where to focus remediation efforts for this specific vulnerability - i.e., in this example it makes sense to remediate the SYN flood to port 443 on the Scrubbing Center.

If the vulnerability is not patched – and this combination arrives – the target (or even the entire IT infrastructure) is likely to be taken down - until there is manual intervention.

Closing Holes that Attackers Love to Exploit

Patching a DDoS vulnerability in the protection solution before an attack succeeds may require multiple adjustments until the mitigations are able to stop the attack automatically.

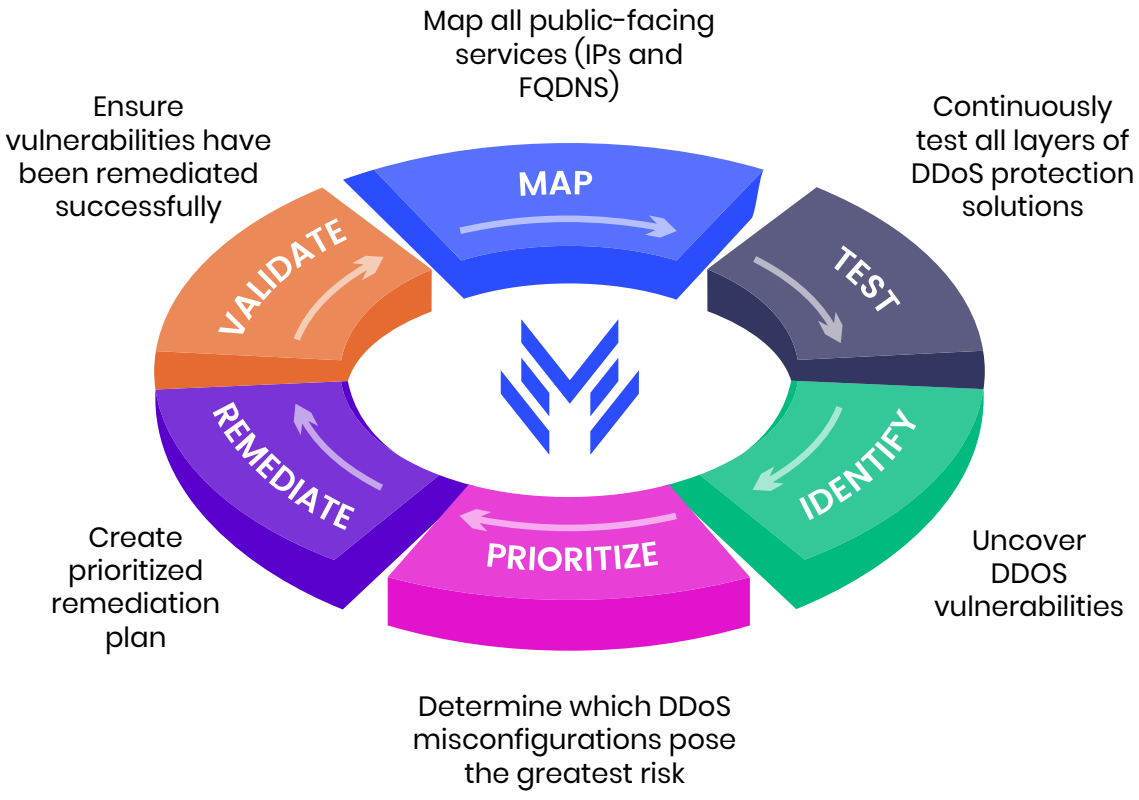
These adjustments may include:



The best way to minimize DDoS vulnerabilities involves:

1. Mapping all public-facing services
2. Proactively testing your organization's automated DDoS protections
3. Identifying all known DDoS vulnerabilities in all defense layers
4. Prioritizing which vulnerabilities pose the greatest risk
5. Remediating vulnerabilities by patching misconfigured policies
6. Validating that those vulnerabilities have been patched

Through this continuous validation, you can ensure that your organization has an optimal solution that is at minimal risk of a successful attack.

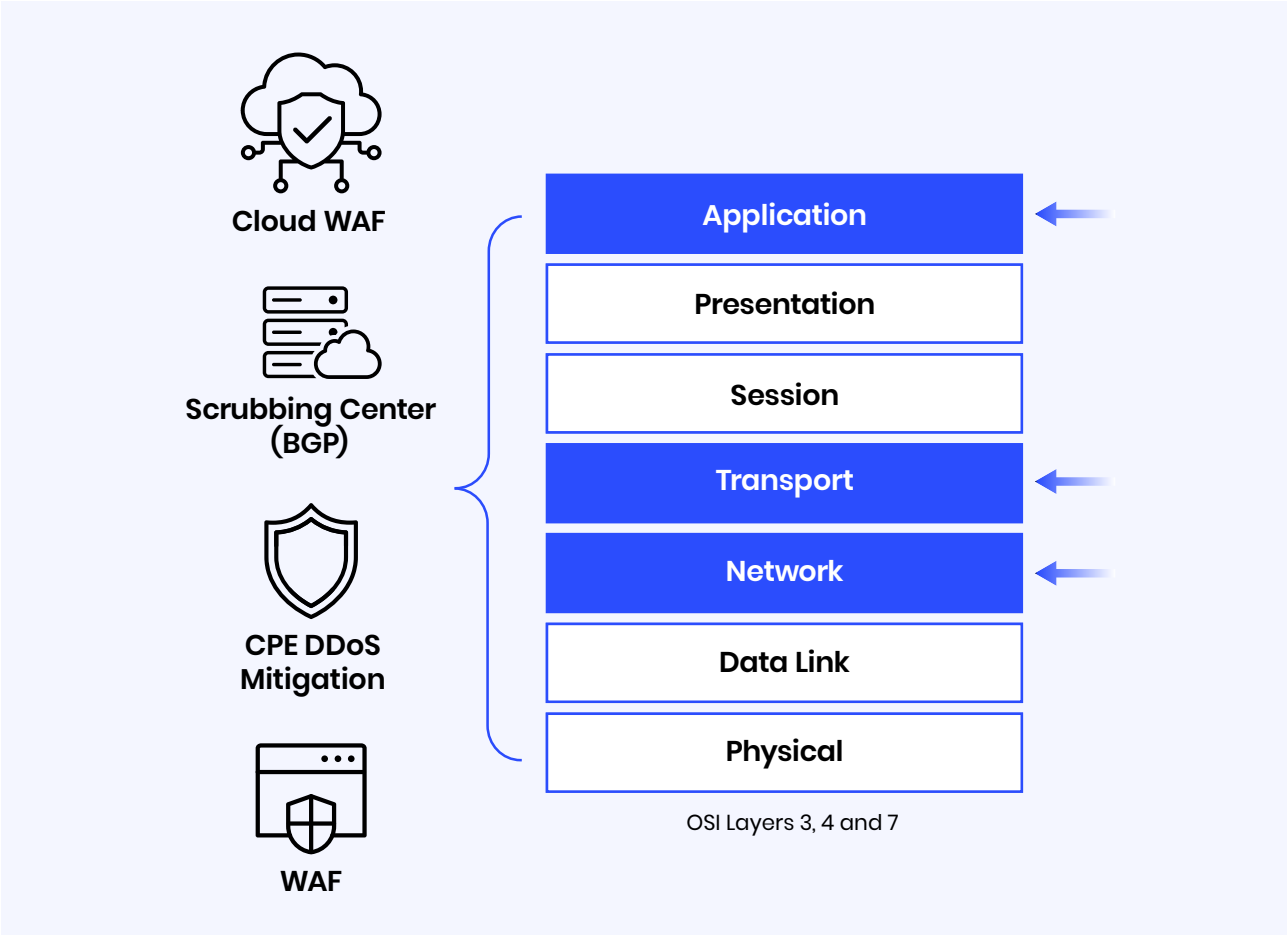


Test and Validate DDoS Protections

The DDoS Reality Check

DDoS vulnerabilities differ from other types of vulnerabilities in several important ways:

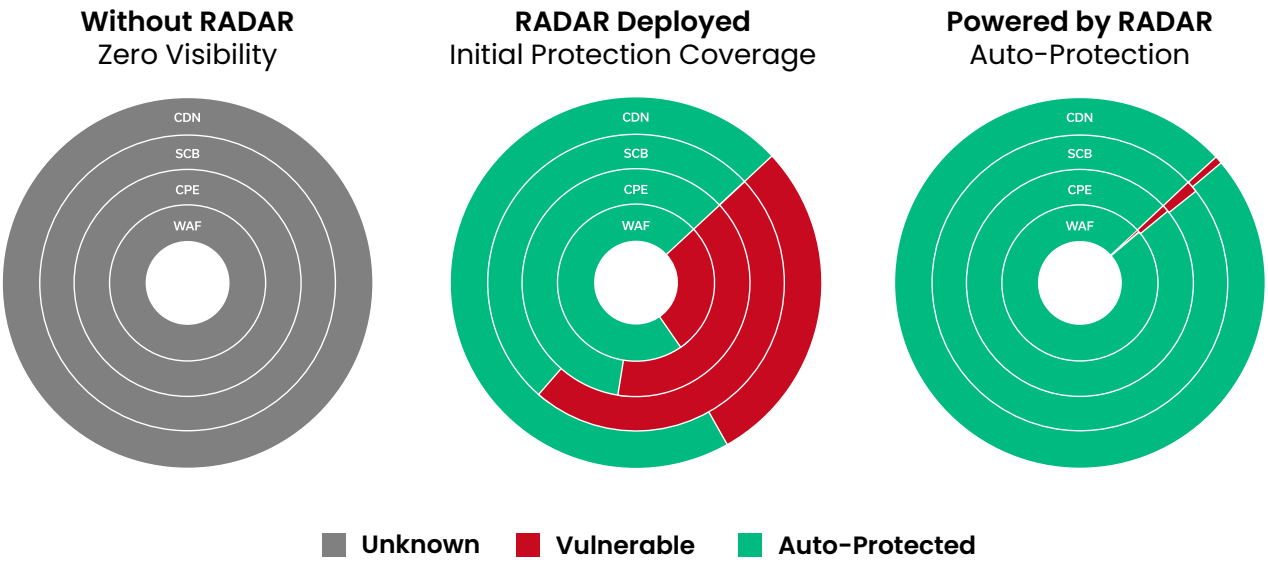
- DDoS security relies on automated DDoS protection to avoid a damaging DDoS attack
- The only reason a DDoS attack succeeds is when the DDoS protections are vulnerable
- Vulnerabilities typically arise naturally from network and service changes leading to protection security policy misconfigurations
- The only place to remediate a DDoS vulnerability is in the specific organization's DDoS protection deployment
- Attack vectors that are most likely to cause damage to a specific environment must be prioritized to ensure the most damaging vulnerabilities are remediated first



Identification of All Known DDoS Vulnerabilities in All Defense Layers

Eliminate the DDoS Protection Gap

MazeBolt RADAR is a patented DDoS testing and vulnerability management solution that runs continuous, nondisruptive DDoS attack simulations. It identifies and enables the remediation of DDoS vulnerabilities that lead to damaging downtime.



RADAR Closes DDoS Protection Gaps

RADAR intelligently prioritizes attack vectors that are most likely to cause damage using the AI-powered SmartCycle™ feature – a new way for even complex enterprises, with the largest attack surfaces, to prioritize DDoS vulnerability remediation.

Global enterprises trust RADAR to proactively prevent damaging attacks, dramatically reducing reliance on reactive manual responses or SLA guarantees. With its unique technology, RADAR provides unparalleled visibility into defense configurations - empowering organizations to prevent DDoS attacks and maintain uninterrupted business continuity.

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.