

What Most DDoS Protection Vendors Don't Want You to Know

7 Inconvenient Truths for the
Financial Sector



Table of Contents

Executive Summary	3
Caught in the Crosshairs - Finance is at High Risk	4
We've Increased Spend - Do We See Less Downtime?	4
New Regulations Raise the Cost of Downtime	5
Common Attack Vectors Will Bring You Down	6
Red Teaming Exposes a Fraction of DDoS Vulnerabilities	7
Triggering an SLA Means the Damage is Already Done	8
DDoS Protections Are Highly Vulnerable without Continuous Attack Simulation	8
Step into the Future! Nondisruptive DDoS Simulation	10
About MazeBolt	11

Executive Summary

The financial industry continues to invest ever-increasing sums in solutions designed to provide protection from distributed denial-of-service (DDoS) attacks. The result is that network security teams try adding new security layers in an attempt to bandage the problem and reduce the risk of damaging DDoS downtime.

But despite attempting to spend their way out of the problem, financial organizations still are being hit. In fact, research indicates a **49 percent increase** in DDoS attacks – with banking and financial services bearing the brunt of these incidents. Each damaging DDoS attack costs close to **half a million dollars**. BFSI enterprises in the US face an average of 25 to 30 DDoS attacks annually; 35-40%, on average,

cause damage such as downtime, financial losses, or reputational harm—resulting in 8 to 12 damaging DDoS attacks per year.

Against this background, using the same reactive approach to solving the DDoS problem just leads to the same results: an inability to successfully thwart DDoS attacks and avoid damaging DDoS downtime. Mitigating the risk successfully requires obtaining a more fundamental understanding of the nature of DDoS vulnerabilities and adopting a new strategy. This eBook dispels some of the misconceptions around DDoS by taking a closer look at why DDoS continues to be one of the top threats to business continuity – and what is necessary to mitigate this threat.



INCONVENIENT TRUTH 1

Caught in the Crosshairs – Finance is at High Risk

Compared to other industries, the financial industry is at particularly high risk of suffering damaging DDoS attacks, due to the critical need for customers to have access to online services 24/7. In the third quarter of 2024, it was the most targeted sector globally for DDoS attacks, according to a report by DDoS protection vendor [Cloudflare](#).

This heightened risk stems from the sector's critical role in the global economy and its reliance on real-time online services. It is an attractive target for cybercriminals aiming to disrupt operations and access sensitive data.

INCONVENIENT TRUTH 2

We've Increased Spend – Do We See Less Downtime?

The threat to operational resilience and business continuity has been growing, as we've seen in the headlines – with a surge of DDoS attacks taking down critical, online services in large, international organizations worldwide, and the average reported cost of a damaging DDoS attack reaching over \$400,000 per attack. Enterprises in finance typically experience about 67 attacks per year.

The situation has been aggravated by:



DDoS as a Service

DDoSaaS makes it even easier for malicious actors to launch large-scale DDoS attacks.



Growing Geopolitical Tensions

Hacktivist groups motivated by political and ideological agendas are driving the current growth in DDoS attacks.



AI as Cyber Disrupter

AI finds DDoS vulnerabilities, giving hackers access to a broader set of attack vectors.

INCONVENIENT TRUTH 3

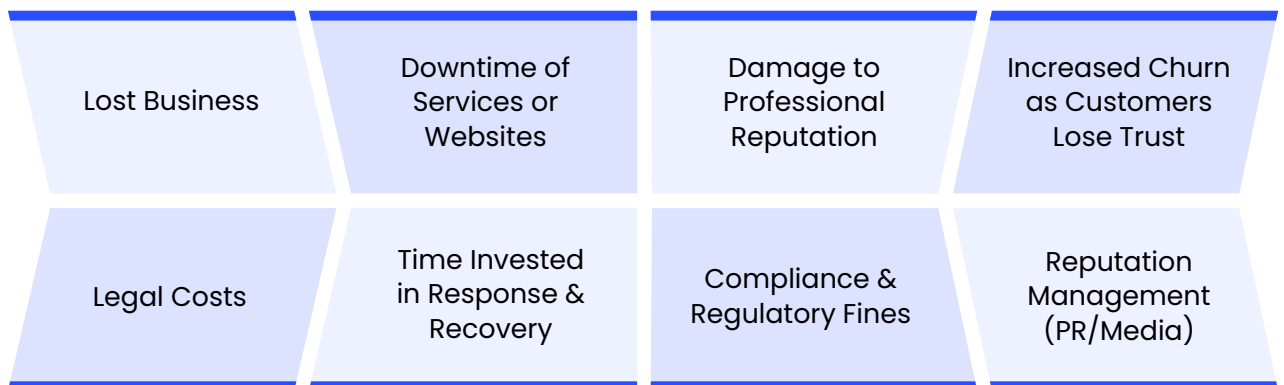
New Regulations Raise the Cost of Downtime

Recent cybersecurity regulations including the [NIS2 Directive](#), [Digital Operational Resilience Act \(DORA\)](#), and [Securities and Exchange Commission \(SEC\)](#) requirements have raised the potential costs with hefty fines for noncompliance. These penalties represent an additional expense, in addition to:

- Direct costs to the business due to downtime
- Potential customer churn
- Operational costs connected to resolving the attack
- Reputational damage to the business

Recent cybersecurity regulations raised the potential costs with hefty fines for noncompliance.

The new regulation requirements mandate continuous risk management and more in-depth reporting. They charge significant fees, adding insult to injury for organizations that have suffered from damaging DDoS downtime. Particularly as the financial services industry is heavily regulated, the compliance requirements provide a compelling incentive to adopt new strategies that mitigate DDoS risk.



Calculating the Total Cost of a DDoS Attack

INCONVENIENT TRUTH 4

Common Attack Vectors Will Bring You Down

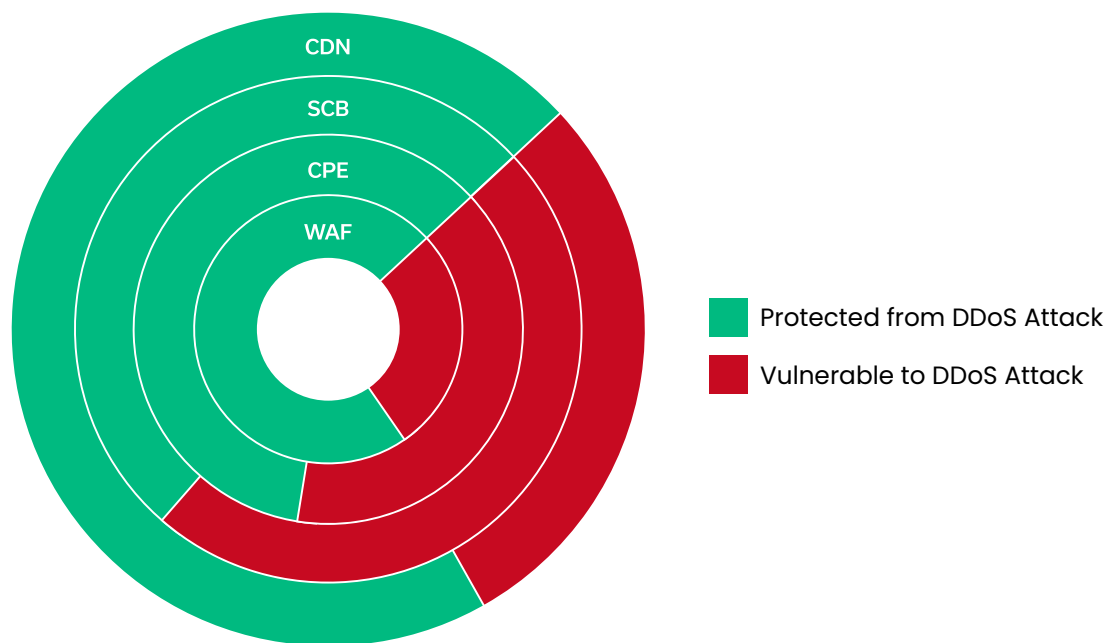
Security leaders need to promote an understanding that the only reason DDoS attacks succeed is due to the existence of vulnerabilities in the DDoS protections being relied on. Typically, vulnerabilities arise from the misconfiguration of DDoS protection security policies.

Vulnerabilities exist because DDoS protections are not configured properly to protect the network and applications, for example:

- New applications were added to the network
- Changes were made to the organization's API
- New ports have been opened in the firewall

DDoS protection solutions require ongoing adjustment to their configurations and settings, to reflect any changes that were made to the network topology and user settings. But typically, the configuration of DDoS protections is not aligned fully with the dynamic and regular changes that are made.

This is what leaves organizations exposed to damaging attacks. According to MazeBolt research, organizations with DDoS protections deployed – even premium protections – typically remain at least 37% vulnerable.

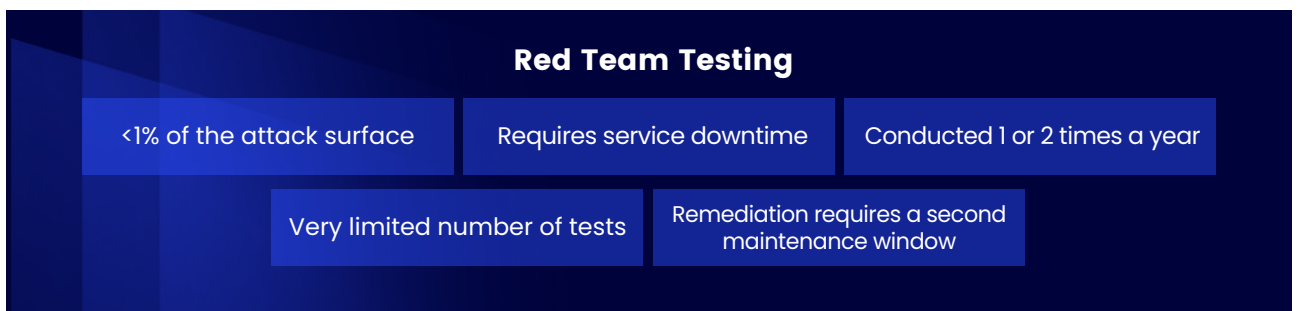


Organizations with DDoS Protections Typically Remain 37% Vulnerable

INCONVENIENT TRUTH 5

Red Teaming Uncovers Only a Fraction of DDoS Vulnerabilities

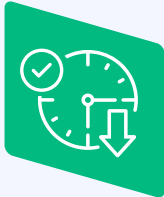
Traditional Red Team testing is designed to validate the effectiveness of DDoS protection solutions. However, Red Team testing usually happens only once or twice a year. Moreover, this approach covers just a small percentage – less than 1% – of the entire attack surface, which includes all public facing services IP and FQDNs.



Limitations of Red Teaming


The primary reason Red Team testing is so limited is because it requires a maintenance window, which disrupts business operations. It requires taking services offline and therefore, it is costly for organizations to implement.

Because of these limitations, even organizations that deploy top-of-the-line DDoS protection solutions lack ongoing DDoS [vulnerability data](#). This means they don't have the necessary visibility that's required to identify and remediate DDoS vulnerabilities.




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

Red Team Testing Exposes a Fraction of DDoS Vulnerabilities

INCONVENIENT TRUTH 6

Triggering an SLA Means the Damage is Already Done

Frost & Sullivan's report on [Ongoing Vulnerability Testing for DDoS Protection](#) points out that DDoS mitigation vendors are limited to acting reactively – only correcting misconfigurations in DDoS protection solutions during or after a damaging DDoS attack. They rely heavily on service level agreements (SLAs) – an approach that puts organizations at a higher risk of downtime.

To counter the growing DDoS risk and stay compliant with regulations, banks and financial services organizations need to complement the reactive approach taken by DDoS protection solutions with a more proactive approach. Some vendors such as [Microsoft](#) and [F5](#) are beginning to understand this more clearly

INCONVENIENT TRUTH 7

DDoS Protections are Highly Vulnerable without Continuous Attack Simulation

Continuous DDoS attack simulation is a must-have enhancement to DDoS protection solutions. By proactively simulating DDoS attacks, continuous DDoS attack simulation validates the effectiveness of DDoS protections. It identifies misconfigurations in these solutions and enables banks and financial services organizations to remediate the risk – by providing prioritized remediation guidance and recommendations.

Adopting continuous DDoS attack simulation allows organizations to:



Prevent
damaging DDoS
downtime



Avoid costly
SLAs



Eliminate
manual SOC
intervention



Stay compliant
with the
regulations

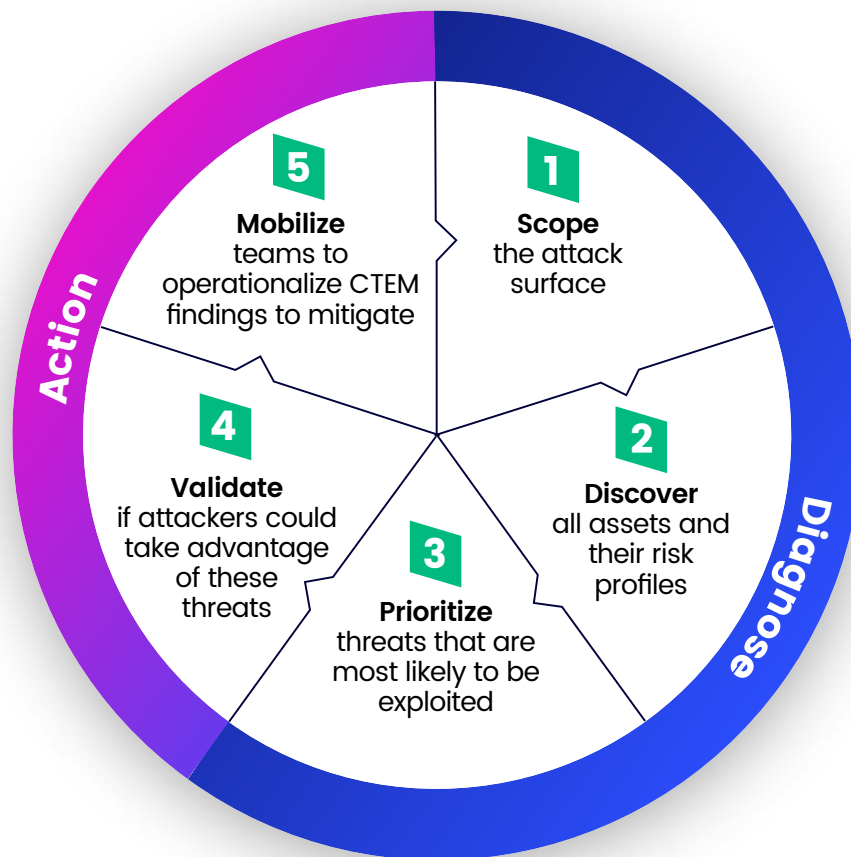
Continuous DDoS attack simulation allows banks and financial services organizations to prevent damaging DDoS attacks completely.

Continuous DDoS attack simulation is aligned with Gartner's [Continuous Threat Exposure Management](#) (CTEM) framework, which calls for continuous DDoS testing for critical online services. To diagnose risk across a complex network infrastructure in line with CTEM principles requires:

Proactively looking for gaps or weaknesses in current DDoS protections

Ensuring no business disruption – no downtime to live environments

Comprehensive reporting and guidance to enable agile mitigation of the highest vulnerability risks



5 Steps in the Cycle of Gartner's CTEM

Step into the Future! Nondisruptive DDoS Simulation

Vulnerabilities in automated DDoS protection solutions are the only reason an organization can suffer from damaging DDoS downtime. (This assumes that DDoS protection solutions were deployed.)

The configuration of DDoS protection security policies, typically, is not correctly maintained or aligned with the ongoing and dynamic changes that have been made to the network. This gap creates vulnerabilities that can be exploited. And if a DDoS attack exploits a vulnerability in the deployed DDoS defenses, it's the customer who suffers damaging downtime.

At a time when financial services are seeing a sharp increase in DDoS attacks, continuous DDoS attack simulation allows financial organizations to optimize DDoS automated defenses proactively – enabling them to find and remediate vulnerabilities before an attack occurs. As a must-have enhancement that complements the capabilities of DDoS protection solutions, continuous DDoS attack simulation allows organizations to protect themselves from damaging DDoS downtime.

Vulnerabilities in DDoS protection solutions are the only reason an organization can suffer from damaging DDoS downtime.

About MazeBolt

MazeBolt RADAR™ is a patented DDoS Vulnerability Management solution. Using thousands of nondisruptive DDoS attack simulations and without affecting online services, it can identify and enable the remediation of vulnerabilities in deployed DDoS defenses. RADAR enables global banking, financial services, and insurance companies worldwide to maintain the uninterrupted business continuity of online services. Using RADAR's patented vulnerability simulation technology, enterprises have unparalleled visibility into their DDoS protection solutions and can stop damaging DDoS attacks – before they happen. Read more at www.mazebolt.com.

