MAZEBOLT

WHITEPAPER

The State of DDoS Mitigation 2018

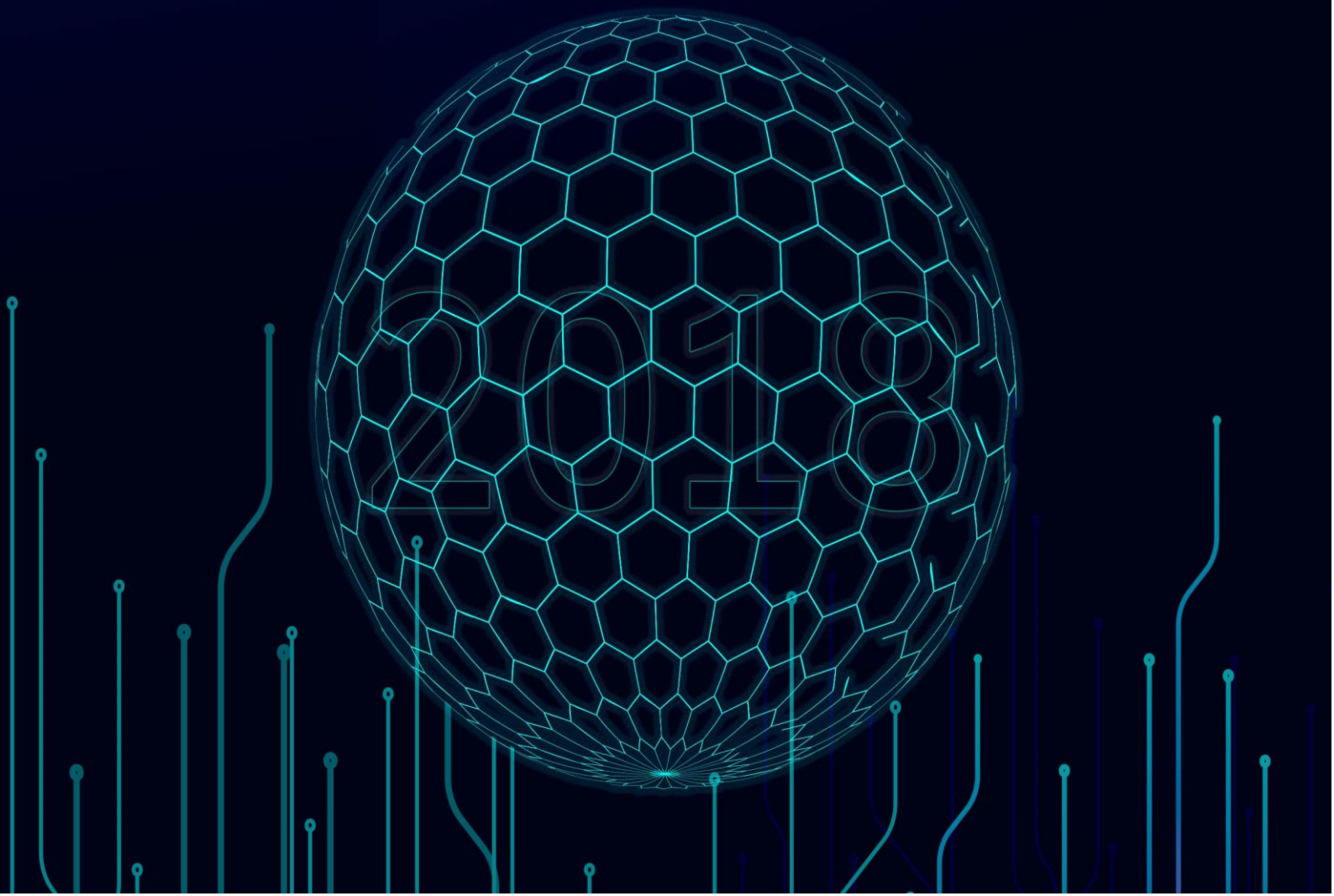


Table of Contents

Table of Figures

Forward – The State of DDoS Mitigation

Matthew Andriani
CEO & Founder
MazeBolt
Technologies

DDoS attacks are having devastating effects on enterprise online operations with a scale that has steadily increased, to a record high of 1.7 Terabits per second. Unfortunately, there doesn't seem to be an end in sight.

It isn't surprising then to learn that according to a study by Neustar, DDoS attacks have become so common that 84% of enterprises report having been *DDoSed* in the past year, and 45% were hit more than 5 times in the same period!

Besides the tremendous financial loss estimated at over US$2M per attack, Neustar found that 92% of organizations that came under attack reported that DDoS attacks were coupled with some additional form of malicious cyber activity adding a whole new dimension of complexity for security teams to deal with.

The data is clear:

DDoS mitigation is not a 'plug & play' solution, it needs continuous fine-tuning to work properly.

In light of this reality, organizations are procuring DDoS mitigation services that are designed to ***identify*** malicious DDoS traffic and ***block*** it ***before*** it reaches their networks.

DDoS mitigation vendors create a wave of quarterly reports that provide a wealth of information about DDoS attacks, their type, size, geographical distribution, frequency and much more …

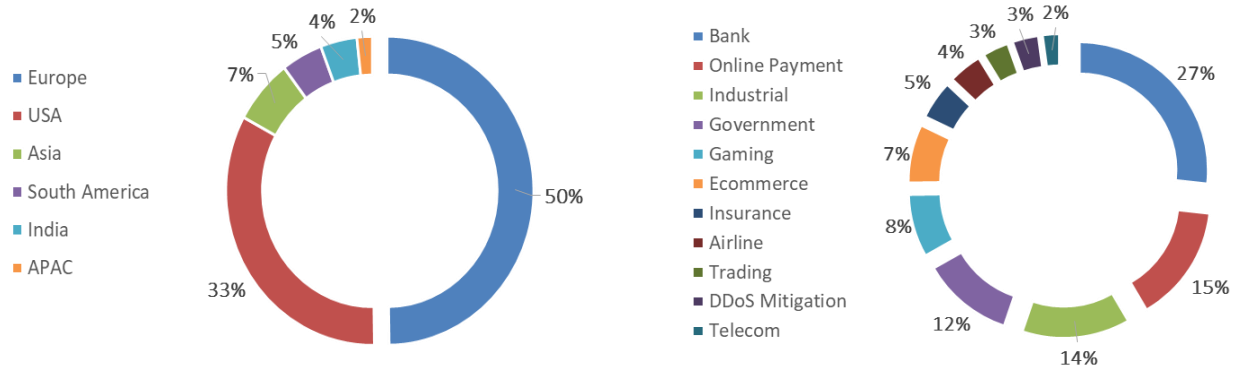
but there is one missing statistic …

… how effective have DDoS mitigation vendors been at actually mitigating these attacks?

This report presents the effectiveness of DDoS mitigation. The data we summarize was collected systematically to provide insight into how well DDoS mitigation *actually works* and what can be done to better protect your organization's operations from the DDoS threat.

The information presented in this study is the first and most comprehensive global study on the performance of DDoS mitigation systems in the enterprise environment. The study is a ***vendor neutral*** analysis based on data collected from over 740 DDoS tests performed over a period of three years covering 2015, 2016 & 2017 with the geographical and industry breakdowns detailed in Figure 1 below.

Figure 1 - DDoS Tests by Region and Tested Industries (%)



What makes this study unique, is that all the DDoS tests were performed in accordance with MazeBolt's BaseLine DDoS testing methodology (For more about BaseLine Testing see Page 13 below). This renders all data points consistent with respect to the DDoS attack vectors, their bandwidth, distribution and test duration and allows a view of DDoS Mitigation systems' performance that has previously been unattainable.

The Bottom Line – Effective DDoS Mitigation Requires Continuous Fine-Tuning

DDoS mitigation technology has the ability to block DDoS attacks. However, when tested for the first time, **97% of enterprises experienced some level of disruption** to their ongoing operations, or complete downtime. For an effective DDoS mitigation posture enterprises need to augment their DDoS mitigation with an effective and efficient way of identifying their points of failure to provide their

DDoS mitigation doesn't work without continued fine-tuning & configuration.

97%

of organizations experienced disruption during 1st DDoS test

DDoS mitigation vendor with the information needed to fine-tune configuration and tighten up their mitigation.

#1 Why is DDoS Mitigation So Difficult to Get Right?

Unlike other network devices such as border Routers or Firewalls, that usually operate smoothly once they are configured, DDoS mitigation is fundamentally different.

An initial configuration for a DDoS mitigation solution, if performed accurately, should automatically protect the downstream network environment from the most common DDoS attacks in the wild.

For DDoS mitigation to continue working properly it needs to be perfectly configured to the specific network it is protecting. The problem is that enterprise networks are constantly changing with servers and services added to networks to meet new demands. In order to ensure that DDoS mitigation is perfectly configured, enterprises need to match each network change with a respective fine-tuning of their DDoS mitigation posture.

In reality, enterprises do not continuously fine-tune and re-configure their DDoS mitigation posture. Over time, this translates into vulnerabilities through which DDoS attack vectors penetrate and hit their network – or in other words a continual *DDoS Gap*.

#2 Managing DDoS Risk – The DDoS Gap

With 84% of enterprises reporting at least one DDoS attack during the past year it comes as no surprise that enterprise IT managers are investing significant resources in their DDoS mitigation postures.

"Most CTOs can't quantify their DDoS risk or show their Executive Management how spending on DDoS mitigation has impacted their ability to mitigate DDoS attacks more effectively."

Matthew Andriani, MazeBolt CEO

The DDoS Gap quantifies the number of DDoS vectors bypassing a company's DDoS mitigation posture

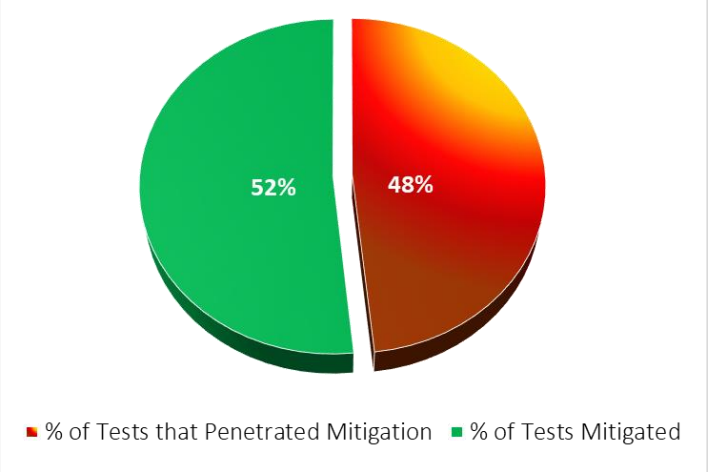
Standardized BaseLine Testing allows enterprises to measure the number of DDoS attack vectors bypassing their DDoS mitigation posture in a quantifiable and easy to understand manner. This establishes the

DDoS Gap as a ***lingua franca*** with which to measure their DDoS risk and communicate it to all relevant stakeholders: from the highly tech savvy IT Security Teams and DDoS mitigation vendors to their non-technical Executive Management. The standardized nature of the DDoS Gap also clearly reflects the effectiveness of a DDoS mitigation posture over time, allows comparison across business units and against industry averages – allowing enterprises to manage their DDoS risk with an effectiveness that has previously been unachievable.

#3 The Initial Industry Average DDoS Gap

BaseLine testing a DDoS mitigation posture for the **first time** defines an enterprise's ***initial*** DDoS Gap, reflecting their susceptibility to the most common DDoS attack vectors.

Figure 2 - Industry Average Initial DDoS Gap (2015 – 2017)



As indicated above, **97%** of the enterprises MazeBolt tested for the first time experienced service disruption or complete down time. The DDoS Gap provides valuable insight into the reasons for these failures in terms of identifying the actual DDoS attack vectors that penetrated the DDoS mitigation postures.

Based on 420 DDoS tests conducted on enterprises ***for the first time*** between 2015 to the end of 2017, the ***Initial DDoS Gap of 48%***, presented in Figure 2, represents the percent of DDoS attack vectors that penetrated the enterprises' DDoS mitigation postures.

... from 2015 to 2017 DDoS mitigation vendors have not been able to consistently improve their mitigation capabilities

Figure 3 - Annual Average Initial DDoS Gap & # of Tests performed

Interestingly when looking at the annual initial DDoS Gap for this period as presented in Figure 3 (with the respective number of tests conducted per year) we see that from 2015 to 2017 DDoS mitigation vendors have not been able to *consistently* improve their mitigation capabilities

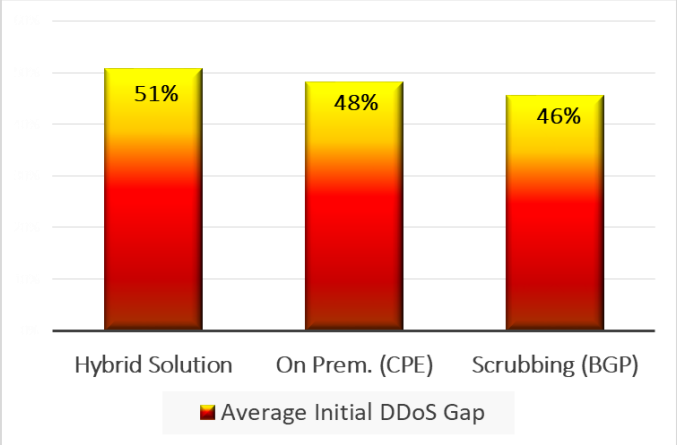
#3.1 Initial DDoS Gap by Mitigation Posture

DDoS mitigation postures come in three basic configurations: On-Prem Devices (a.k.a. Customer Premise Equipment or "CPE"), Cloud Scrubbing Services and Hybrid solutions that combine both On-Prem Devices and Scrubbing (BGP) Services.

Figure 4 - Average Initial DDoS Gap by DDoS Mitigation Posture (2015 – 2017)

Figure 4 presents the average initial DDoS Gap for 2015 – 2017 by type of DDoS mitigation posture with the respective number of tests performed during this period.

All three DDoS mitigation postures are significantly vulnerable with DDoS Gaps ranging from 48% (On-Prem) to 40% (Scrubbing Services).



While the average for 2015 – 2017 reflects similar performance for all three DDoS mitigation postures, looking at 2017 alone highlights a significant improvement for Scrubbing Services (BGP)

Looking at the performance of each of the DDoS mitigation postures on an annual basis, Figure 5 below shows how from 2015 to 2016 the generally improved performance reflected in a decreasing initial DDoS Gap deteriorated in 2017 with rising DDoS gaps for all three mitigation postures.

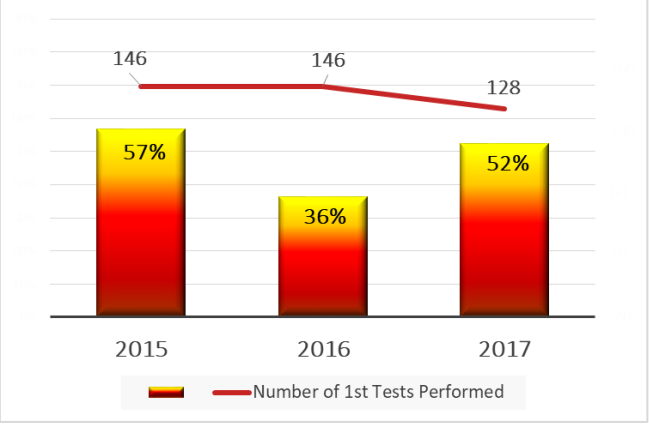
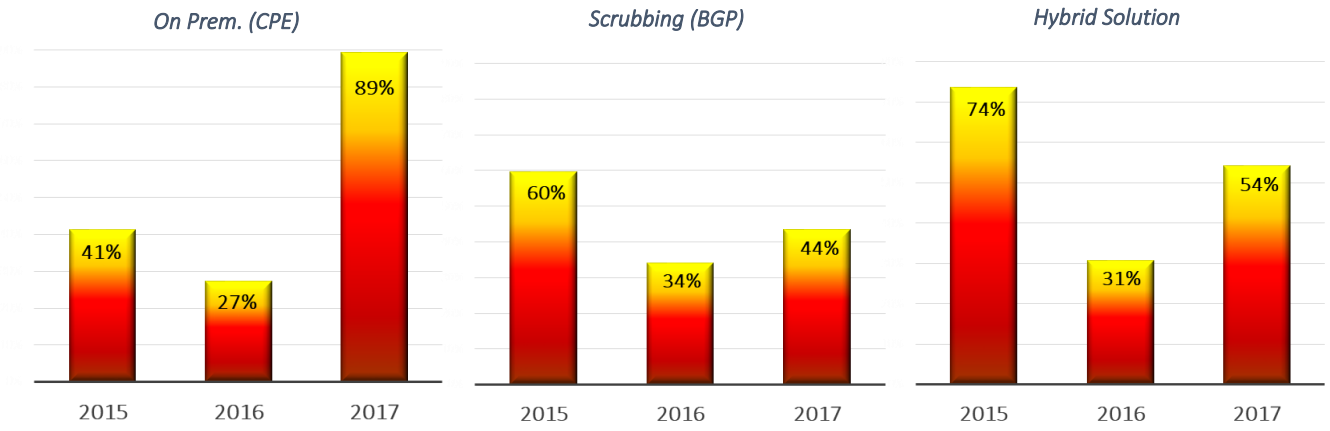


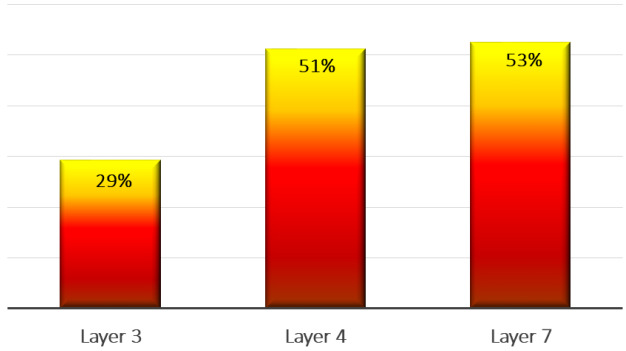
Figure 5 - Average Initial DDoS Gap (2015 - 2017) by type of mitigation



#3.2 Initial DDoS Gap by DDoS Attack OSI Layer

DDoS attacks hit networks on three different Open Systems Interconnection (OSI) Layers: *Layer 3* (Network), *Layer 4* (Transport) and *Layer 7* (Application).

Figure 6 - Average Initial DDoS Gap by OSI Layer (2015 – 2017)



While each OSI layer has its different characteristics, Layer 3 & Layer 4 DDoS attacks are typically characterized as high bandwidth and low complexity attacks. Examples of Layer 3 & Layer 4 DDoS attacks are the high-profile attacks that hit Dyn @1.2Tbps, OVH @ 1Tbps in 2016 and Github @ 1.35Tbps in 2018.

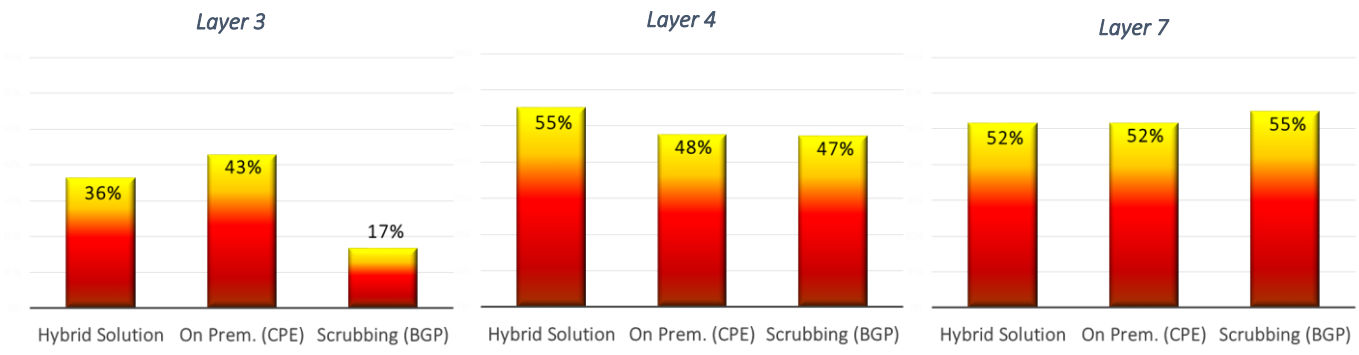
Layer 7 attacks, on the other hand, are typically low bandwidth and higher complexity, which generally makes them more difficult to identify and mitigate.

From the average initial DDoS Gaps for 2015 – 2017 by DDoS attack OSI Layer (depicted in Figure 6) it is clear that DDoS mitigation is most effective against Layer 3 attacks and are generally less successful when it comes to Layer 4 & Layer 7 Application attacks.

From 2015 to 2017 Scrubbing Services were better at mitigating Layer 3 & Layer 4 attacks, while Hybrid Solutions showed the best mitigation for Layer 7 Attacks

Looking at the initial DDoS Gap by OSI Layer from the perspective of the three DDoS Mitigation postures shows that Scrubbing Services have been better at mitigating Layer 3 & Layer 4 attacks, while Hybrid solutions have been the best at mitigating Layer 7 Attacks.

Figure 7 - Average Initial DDoS Gap 2015 – 2017 by OSI Layer and type of DDoS mitigation posture



#3.3 Initial DDoS Gap by DDoS Attack Vector

Drilling down into the effectiveness of DDoS mitigation to block actual DDoS attack vectors, provides us with the most difficult DDoS attack vectors to mitigate – listed in Figure 8 by year for 2015, 2016 & 2017.

Figure 8 - The 10 Most Difficult DDoS Attack Vectors to Mitigate for 2015, 2016 & 2017

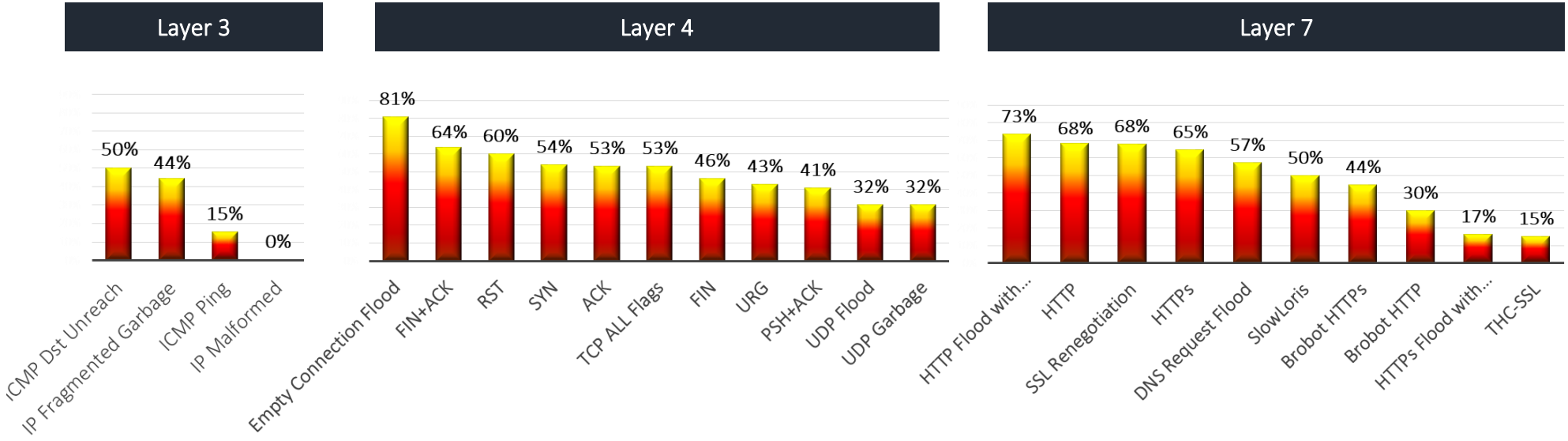
Figure 9 takes an overview for the entire period (2015 – 2017) and groups the DDoS attack vectors by OSI Layer for convenience. The DDoS attack vectors in each Layer are presented in decreasing order from left to right

2015		
#	DDoS Attack Vector	DDoS Gap
1	Brobot HTTPs	100%
2	HTTPs	100%
3	SSL Renegotiation	86%
4	Empty Connection Flood	75%
5	FIN	67%
6	HTTP	67%
7	HTTPs Flood with Browser Emulation	67%
8	ICMP Dst Unreach	67%
9	HTTP Flood with Browser Emulation	63%
10	PSH+ACK	63%

2016		
#	DDoS Attack Vector	DDoS Gap
1	HTTP Flood with Browser Emulation	71%
2	FIN+ACK	60%
3	Empty Connection Flood	58%
4	HTTP	50%
5	HTTPs Flood with Browser Emulation	50%
6	ICMP Dst Unreach	50%
7	Multivector attack	50%
8	SSL Renegotiation	50%
9	IP Fragmented Garbage	47%
10	ACK	43%

2017		
#	DDoS Attack Vector	DDoS Gap
1	TCP ALL Flags	100%
2	HTTP	88%
3	HTTPs	82%
4	Empty Connection Flood	75%
5	HTTP Flood with Browser Emulation	75%
6	FIN+ACK	67%
7	SSL Renegotiation	67%
8	DNS Request Flood	60%
9	SlowLoris	57%
10	SYN	57%

Figure 9 - Average Initial DDoS Gap 2015 – 2017 by DDoS Attack Vector



#4 Closing the DDoS Gap

The DDoS Gaps presented so far in this State of DDoS Protection Report for the years of 2015 – 2017 reflect enterprises' DDoS Gaps from the *first BaseLine DDoS Tests*. Understanding their initial DDoS Gap empowers enterprises to work with their DDoS mitigation vendors to fine-tune and fix the configuration issues identified during testing to close their DDoS Gaps and strengthen their mitigation.

Figure 10 - Average Initial DDoS Gap for 2015 – 2017 by # of BaseLine Tests

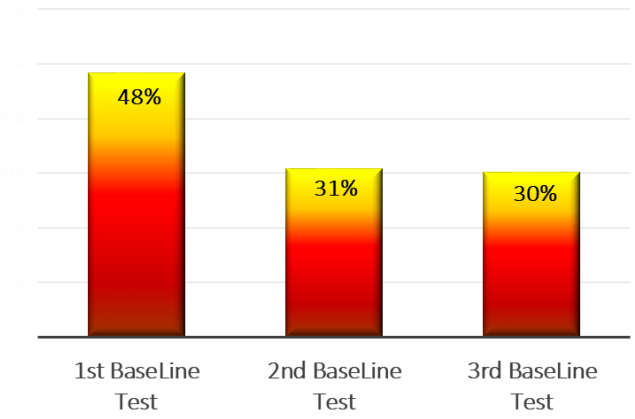


Figure 10 presents the average DDoS Gaps according to the number of BaseLine DDoS tests enterprises completed.

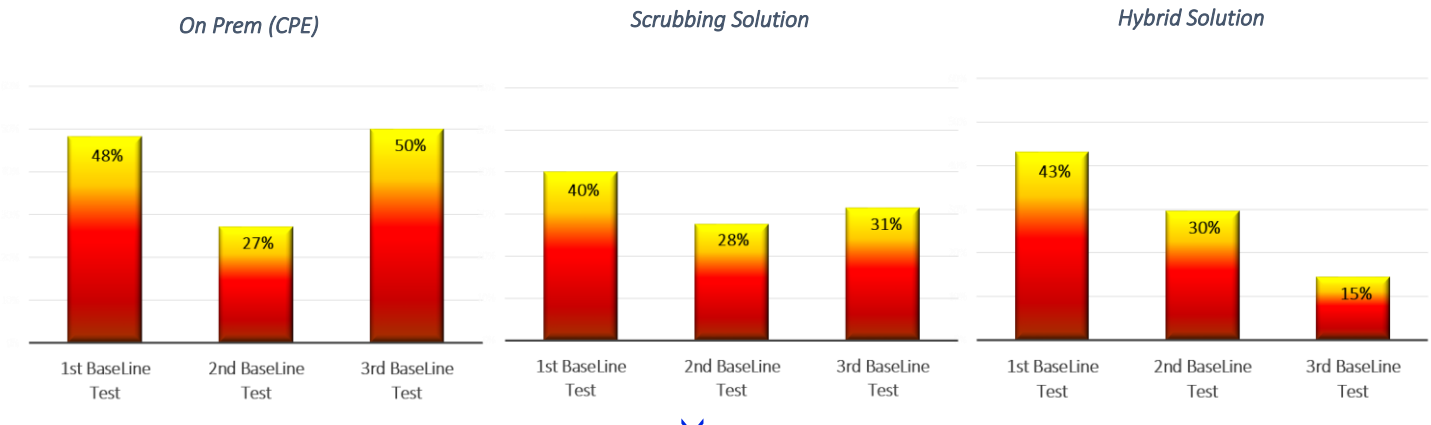
The average DDoS Gap for 2015 – 2017 according to the number of BaseLine DDoS tests enterprises completed by type of DDoS mitigation posture is presented below in Figure 11. Of the three types of DDoS mitigation postures, *Hybrid Solutions* were the most successful in strengthening their DDOS Gap.

65%

*Average Improvement in DDoS Gap for **Hybrid Solutions** after three BaseLine Tests.*

Enterprises were able to strengthen their DDoS Mitigation by over 35% on average in just two BaseLine Tests.

Figure 11 - Closing the DDoS Gap – DDoS Gap by Type of Mitigation Posture

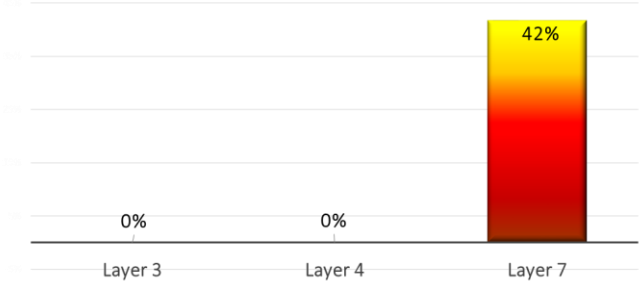


#5 Content Distribution Networks (CDN)

A content delivery network (CDN) is designed to help companies serve their web content to a global audience faster, more efficiently and reliably. While some CDNs do have DDoS mitigation capabilities, some may not, either way, a properly configured CDN by design helps protect companies from DDoS attacks that target their URLs e.g. www.mazebolt.com (CDNs do not mitigate DDoS attacks that target source IP addresses directly).

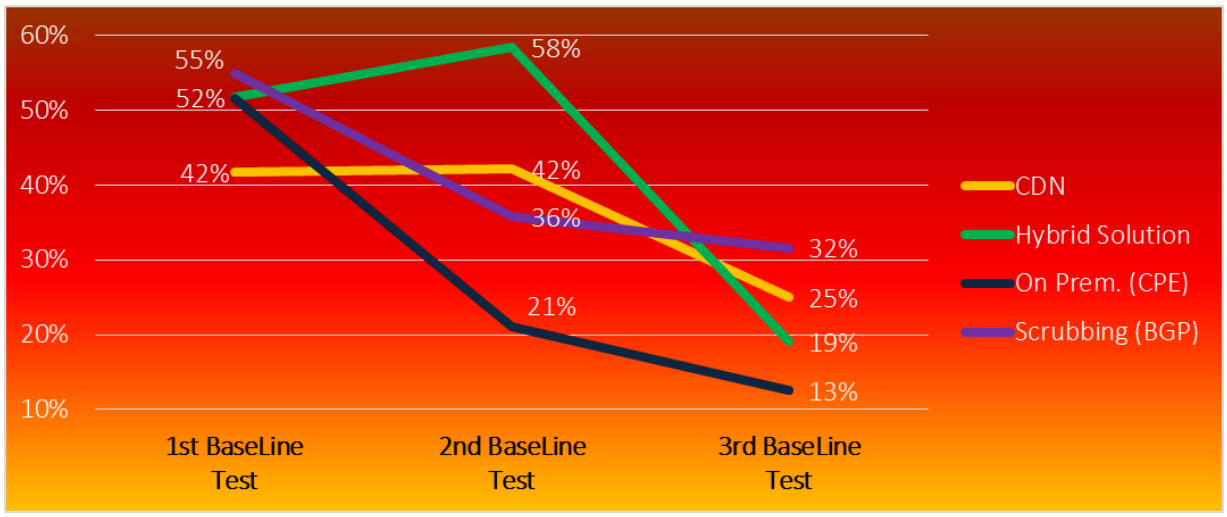
This section presents results from over 180 DDoS tests conducted between 2015 – 2017 in which customers tested their CDNs (Not BGP routing or CPE equipment) only by targeting their FQDN names and not source IP addresses. This means that all DDoS test traffic had to first pass through the CDN infrastructure and not directly to the source IP. As illustrated in Figure 12 CDNs are inherently vulnerable to Layer 7 attacks. While the initial DDoS Gap for Layers 3 & 4 DDoS Tests was zero, the initial CDN DDoS Gap for Layer 7 was 42%.

Figure 12 - CDN Average Initial DDoS Gap 2015 – 2017 by OSI Layer



Comparing between CDN Layer 7 mitigation and the performance of dedicated DDoS mitigation solutions, as illustrated in Figure 13 below, shows that initial CDN mitigation of Layer 7 (After the 1st BaseLine Test) is the most effective. However, when Layer 7 mitigation is viewed over three BaseLine Tests, we see that both CPE & Hybrid solutions show stronger improvement on average and dedicated CPE have the best results in Layer 7 mitigation as more testing completed.

Figure 13 - Average Layer 7 DDoS Gap by Type of Mitigation & # of BaseLine Tests Completed



Appendix: Report Introduction & Overview

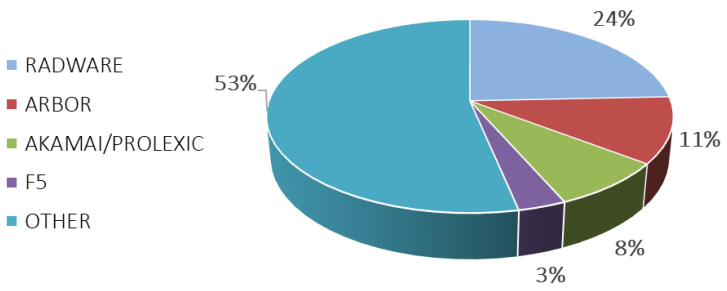
A word on DDoS Mitigation Vendors & Maintaining Vendor Neutrality

MazeBolt's DDoS Testing is vendor neutral.

To avoid the appearance of bias towards any of the vendors the report only provides aggregated data at the industry level, Figure 3 details the volume of testing per mitigation vendor.

Without exception, vendors were found to be vulnerable to MazeBolt's BaseLine Tests and they all needed configuration fine-tuning to strengthen their technology.

Figure 14 - Mitigation Vendors' Share of Testing



Other* - The vendor either accounted for less than 3% of total tests performed or was not disclosed by the end customer.

What is BaseLine DDoS Testing?

Standardizing DDoS Tests: MazeBolt's BaseLine DDoS test is designed to verify that a DDoS mitigation posture can automatically mitigate over 95% of the most common DDoS attack vectors in the wild.

Mapping Attack Vectors To Mitigation Mechanisms: With hundreds of DDoS attack vectors in the wild, testing a mitigation posture against them all is just not feasible. Therefore, MazeBolt has "flipped the question" and focused instead on verifying that the main mitigation mechanisms

Figure 15 - Baseline DDoS Tests – Mapped to Main Mitigation Mechanisms & OSI Layers

#	Layer	Attack Type	Mitigation Mechanism Tested
1.	3	IP Fragmented Flood	- Behavioral - Signature - L4 Challenge - Out of state
2.	3	ICMP Flood	
3.	4	UDP Flood	
4.	4	UDP Garbage Flood	
5.	4	URG Flood	
6.	4	Empty Connection Flood	
7.	4	PSH+ACK Flood	
8.	4	ACK Flood	
9.	4	RST Flood	
10.	4	FIN Flood	
11.	7	HTTPs Flood	- Layer 7 Challenge - Signature
12.	7	HTTP Flood	
13.	7	Brobot HTTP	
14.	7	Brobot HTTPs	
15.	7	HTTP/s With Browser	
16.	7	SlowLoris	
17.	7	SSL Renegotiation Attack	
18.	7	THC-SLL Attack	

responsible for mitigating over 95% of DDoS attack vectors are working as expected. The BaseLine Test's attack vectors have been chosen to map to the main DDoS mitigation mechanisms (See Figure 4). The BaseLine Testing methodology verifies that the mitigation mechanisms are working automatically, regardless of whether the organization is using On-premise mitigation, Cloud Scrubbing center services or a hybrid solution of the two.

Standardized DDoS Test Results

Enterprise environments respond to DDoS tests in various ways, from immediate down time, to no impact at all. To allow for an accurate comparison of DDoS test results over time and across different network environments, MazeBolt's BaseLine DDoS Testing methodology established a set of DDoS test result metrics.

Figure 16 - MazeBolt's Standard DDoS Test Result Metrics

Test Result	Description
PASS	1. The site/service and network devices were not affected. Mitigation was automatic.
	2. Passed overall, the site/service did not go down straight away; however, some network devices may have been affected and there may have been intermittent slowdown or downtime.
FAIL	1. The site/service went down immediately and network devices may have been affected. However after some time the attack may have been mitigated. Mitigation was either delayed or manually applied. 2. If the site or service being tested was mainly down.
	3. The site went down and stayed down, there was no mitigation throughout the test.

DDoS mitigation (if configured correctly) is based on defense mechanisms that should be able to automatically block the most common DDoS Attack vectors **without requiring any 'human' intervention** i.e. manual changes.

This automatic DDoS mitigation capability is a critical factor that translates into minimal disruption to the target organization's online services and IT infrastructure when under attack.

MazeBolt's DDoS test results' metrics were defined as objectively as possible on the basis of automatic mitigation as detailed in Figure 17:

Ensuring Testing Consistency and Data integrity

Realistic DDoS Tests – Production Environments & Source IPs: The information presented in Sections 1 – 4 of this report is only from DDoS tests that targeted IP's in customers' production environments directly. Customer that requested we only test their FQDN names to ensure we never come directly to their source IP (Likely because they had DNS protection via CDN only) are presented separately in Section 5.

Consistent BaseLine DDoS Testing: The data in this report only includes test results from MazeBolt's Standard BaseLine DDoS Testing methodology. All custom DDoS testing or Advanced Persistent Testing (APT) was not included. E.g. Data from customers who requested testing other than our standard BaseLine Testing Methodology was left out.

Note: Section 3.3 only, (Initial DDoS Gap by DDoS Attack Vector) also presents results from DDoS tests that are not part of the default BaseLine DDoS Attack Vectors

Consistent Network Environment Setups: To insure consistency across different Network Environment setups, test result data was only included in this report if there were a minimum of 30 data points from the same testbed.

About MazeBolt

MazeBolt introduces a new standard in DDoS coverage, automatically detecting, analyzing, and prioritizing remediation across the network, doubling coverage, and virtually eliminating DDoS exposure without shutting down organizational operations. MazeBolt's continuous defense supercharges the performance of CISOs as well as the mitigation service provider.

Traditional DDoS Testing:

The commonly available DDoS Testing technology that is disruptive to ongoing operations and requires maintenance windows. MazeBolt's traditional BaseLine DDoS Testing Methodology – the *de-facto* industry standard – is the most effective method of traditional testing that provides validation of over 95% of all DDoS attack vectors in just 3 hours.

NEW DDoS RADAR™ – "Revolutionary Non-Disruptive DDoS Testing":

Working with any mitigation solution installed, RADAR™ offers superior DDoS coverage and automated DDoS protection. RADAR™ simulates over 100 attack vectors with all public facing IPs 24/7, giving real time visibility to all DDoS vulnerabilities with zero downtime.

