Sep 15th 2016 version

`

RED BUTTON

DDoS Experts

DDoS Vendor Review

Evaluate and select the best solution for your needs

Legal Notice

Red Button and the Red Button logo are trademarks of Red Button Ltd. ("Red Button"), in Israel and other countries. All other brand names, product names, or trademarks are the property of their respective owners.

This DDoS Vendor Review (the "Report" or "DDoS Vendor Review") is proprietary to Red Button, and constitutes valuable intellectual property of Red Button, protected by applicable copyright and trade secret laws and by international treaty provisions. The downloader of the Report is authorized to use this Report and any of the information in this Report, solely for his or her own internal use, and subject to the terms and conditions, including disclaimers, provided herein. No part of this Report may be downloaded, transmitted, broadcasted, transferred, assigned, reproduced, stored in a retrieval system, or in any other way used or otherwise disseminated in any form to any person or entity, without the explicit prior written consent of Red Button, which may be given by way of specific notice displayed on Red Button's website. All unauthorized reproduction or other use of the Report shall be deemed willful infringement(s) of Red Button’s copyright and other proprietary and intellectual property rights. You acknowledge and agree that you will not use the Report in any manner that violates or misappropriates or could result in a violation or misappropriation of intellectual property rights of Red Button, including, without limitation, copyrights, trademarks, and/or trade secrets. Red Button expressly reserves all rights in connection with its intellectual property.

Disclaimer

This DDoS Vendor Review has been developed by Red Button in good faith with the aim to help organizations select the best DDoS Security product for them, and with an effort to provide up-to-date and accurate information on the reviewed products. However, Red Button assumes no liability or responsibility whatsoever for any errors, omissions or inaccuracies in the Report, including in its conclusions and recommendations, and makes no commitment to update the Report. The Report is provided on an “AS IS” basis, without any warranties or representations whatsoever, expressed or implied, and you expressly acknowledge and agree that your use of the Report is at your own risk. Red Button reserves the right to update or revise the Report at any time without notice.

Table of Contents

Introduction

VERSION 1

The need for DDoS Vendor Review and Competitive Analyses

More and more organizations nowadays understand the critical need for DDoS protection. DDoS mitigation products and services may at first glance appear as though they are easy to consume – but they are not. Sadly, many organizations don't understand this until the first severe attack reaches their doorstep and gets their full attention.

There are already solid vendors and service providers promising to immunize you completely from this headache. The good news is that many of them are not bad at all, and most of them have been operating for five to ten years. The bad news is that none of them provides complete, fully automated, fully managed, stable-as-a-rock protection. Each vendor has advantages and disadvantages, and while one vendor can be a perfect match for a given organization, it can be a worse match for another.

There is no question that there is a knowledge gap and that many organizations still do not understand what DDoS is all about, nor do they understand the complexity of this domain and the difference between vendors. **The objective of this document is to assist you with the vendor comparison process.**

Reviewed Products

This report covers the following vendors:

f5 CLOUDFLARE IMPERVA INCAPSULA

Only three products were selected to begin, but the intention is to continue adding vendors in the future.

Methodology

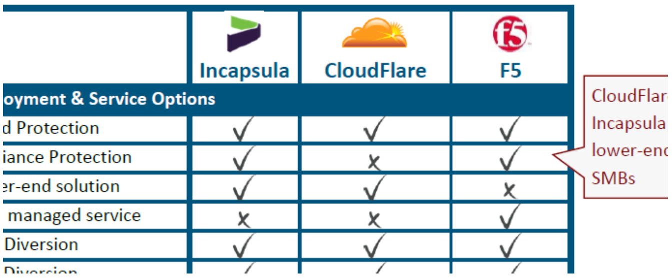
A detailed account of the methodology used can be found in the Research Methodology section. In short, the approach is a technical one.

How to Read this Report

The report includes several sections that compare DDoS vendors from different angles based on technical features and the requirements of different organizations.

Technical Evaluation

The first Technical Evaluation section drills down to compare the deployment options, mitigation capabilities, user experience and reporting of each solution.



	Incapsula	CloudFlare	F5
oyment & Service Options			
d Protection	✓	✓	✓
iance Protection	✓	x	✓
er-end solution	✓	✓	x
managed service	x	x	✓
Diversion	✓	✓	✓
Diversion	✓	✓	✓

CloudFlar
Incapsula
lower-enc
SMBs

Needs-Based Comparison

This section lets you compare the vendors based on your needs, such as the type of protection required or the size of your company. It includes the following comparisons:

- Enterprise Web & Infrastructure Protection. Read this comparison if you require a full-scale DDoS solution that includes protecting both your web services using Web Protection and your network using Infrastructure Protection, if you are considering a fully managed service and if you may also be considering appliance protection in addition to the cloud-based protection. Solutions like this will cost 50-100K USD and can easily cost much more than that. This section compares F5 Silverline with Incapsula Enterprise.
- Enterprise Web Protection. Read this comparison if you require web protection and do not necessarily need Infrastructure Protection, but are sensitive to site performance. This section compares CloudFlare Enterprise with Incapsula Enterprise.
- SMBs. If you are limited by budget and your DDoS requirements include web protection and CDN/site acceleration, read this section, which compares Incapsula Business with CloudFlare Business.

Individual Vendor Review

Read in-depth evaluations of individual DDoS vendors to learn about each vendor’s strengths and weaknesses, background and business focus. This section covers:

- Incapsula
- F5
- CloudFlare

Technical Evaluation

The technical evaluation of vendors is split into three categories: Deployment options, mitigation capabilities, and user experience (UX). The following table provides a top-level summary of all three categories; a detailed analysis can be found in each of the following sections.

	Incapsula	CloudFlare	F5
Deployment & Service Options			
Cloud Protection	✓	✓	✓
On-premises Protection	✓	✗	✓
Web Protection (DNS diversion)	✓	✓	✓
Infrastructure Protection (BGP diverstion)	✓	✓✗	✓
Fully Managed Service	✗	✗	✓
Non-Web Protocols Support	✓	✗	✓
Number of POPs	30	86	4
SMB Plans	✓	✓	✗
Overall Deployment Score	**72%**	**69%**	**65%**
Mitigation Completeness			
Reverse Proxy & Caching	✓	✓	✓
Web Challenges	✓	✓✗	✓
Signatures	✓	✓	✓
Blacklist / Whitelist	✓	✓	✓
Rate Limit	✓	✗	✓
DNS Protection	✓	✓	✓
Overall Mitigation Score	**96%**	**73%**	**100%**
UX & Reporting			
Look and Feel	Excellent	Good	Basic
Easy of Navigation	Excellent	Excellent	Good
Security Configuration	Good	Basic	Basic
Security Events	Excellent	Good	Excellent
Forensics	Basic	Basic	Excellent
Overall UX and Reporting Score	**77%**	**69%**	**65%**

Figure 1: Technical Evaluation Analysis Summary

F5 offers fully managed service.

CloudFlare mitigation is solid, but Incapsula and F5 are much more mature.

Incapsula User Experience (UX) is excellent, CloudFlare is also very good, F5 is basic.

On top of their Enterprise plan, CloudFlare and Incapsula offer lower-end plans for SMBs. See SMB Section

F5 has excellent DDoS Forensics.

A Word on Pricing

Pricing is obviously a major factor in selecting a vendor. Where possible we added the pricing of the portrayed services including pricing of SMBs plans and naked pricing factors for F5 and

Incapsula. Unfortunately, vendor do not will to share their Enterprise prices and you will need to toil and get a quote from each one.

Deployment & Service Options

This section compares the cloud-based and appliance-based deployment options provided by vendors. This section, more than any other, contains items that are "deal breakers" for the customer and can scope out a vendor.

Cloud Deployment

	Incapsula	CloudFlare	F5
Diversion Method: DNS			
Always-on	✓	✓	✓
On-demand	✓	✓	✓
Non-web protocols	✓ (IP Protection)	✗	✓ (L4 proxy)
Diversion Method: BGP			
Always-on	✓	✓✗	✓
On-demand	✓	✓	✓
Service Features			
SSL support – HSM	✗	✗	✗
Emergency response	✓	✓	✓
Fully managed service	✗	✗	✓
Number of data centers	**30** see locations	**86** see locations	**4** San Jose, CA US Ashburn, VA US Frankfurt, DE Singapore, SG
Entry Level			
SMB plans	✓	✓	✗

Figure 2: All-in-All Comparison – Cloud Deployment

Both vendors support non-web protocols.

F5 offers fully managed service.

If you have acceleration needs, F5 is likely to be ruled out.

F5 and Incapsula offer a plan for SMBs.

Diversion Methods

When using a cloud-based protection service, the first question you should ask is how will your traffic traverse your provider data centers (or scrubbing centers, in DDoS jargon)? The first method is DNS diversion, also referred to as web protection. Another method is BGP diversion, also called infrastructure protection. F5 and Incapsula fully support these diversion methods. CloudFlare also claims to support it, but we did not have sufficient data to validate its extent.

There is another more specific diversion method for non-web protocols that only Incapsula and F5 support.

Service Features

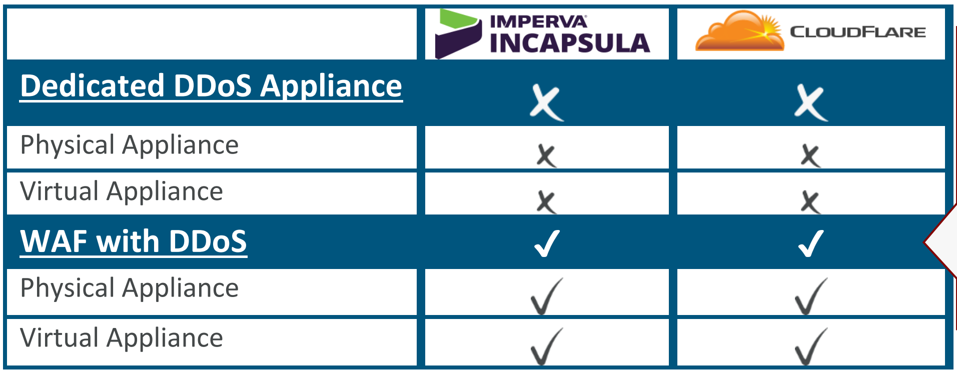
Service level options are critical evaluation criteria for many organizations. When under attack ('War Time'), all vendors will assume full responsibility and provide emergency response. In 'Peace Time,' CloudFlare and Incapsula mostly rely on self-service, whereas F5 provides fully managed service.

The number of data centers can be essential. If you want the service to give you acceleration, only CloudFlare and Incapsula offer a CDN with 86 and 30 POPs, respectively. Even if improving acceleration is not a goal, it is still an advantage because it ensures that you will not suffer any performance degradation. It can also be important for regulatory compliance, for example, in cases in which you cannot use a POP outside your own country.

Entry Level

Budget is always a critical factor. If you cannot spend more than 5,000 USD annually on DDoS mitigation, only the CloudFlare Business and Incapsula Business plans targeting SMBs are suitable. (See more under the SMBs section.)

Appliance Deployment



	IMPERVA INCAPSULA	CLOUDFLARE
Dedicated DDoS Appliance	✗	✗
Physical Appliance	✗	✗
Virtual Appliance	✗	✗
WAF with DDoS	✓	✓
Physical Appliance	✓	✓
Virtual Appliance	✓	✓

Both F5 and Imperva/Incapsula offer DDoS mitigation features on top of their WAF appliances: F5 with ASM and Imperva with SecureSphere.

Figure 3: Technical Evaluation - Appliance Deployment

Another way to implement DDoS mitigation is to use appliances: physical or virtual, DDoS dedicated or as a feature inside WAF or IPS. The report does not cover appliances, but it is important to know which vendor has them in case you go for a hybrid approach. F5 offers ASM (Application Security Module), while Imperva Incapsula offers Imperva SecureSphere. Both are WAF (Web Application Firewall) with DDoS capabilities.

Mitigation

DDoS mitigation capabilities are the core of your decision. All vendors can block the majority of DDoS attacks. Nevertheless, there are some differences that are covered below. CloudFlare has significant security gaps because it lacks Rate Limit and its web challenges type is partial.

	Incapsula	CloudFlare	F5
Proxy / Caching			
Reverse Proxy	✓	✓	✓
Caching	✓	✓	✓
Web Challenges			
Cookie Validation	✓	✗	✓
JavaScript Challenge	✓	✓	✓
Silent Bot Detection	✓	✗	✓
Modern CAPTCHA	✗	✓	✓
CAPTCHA	✓	✗	✓
Signatures			
Vendor	✓	✓	✓
Customer	✓	✓	✓
Blacklist (BL) / Whitelist			
BL IP	✓	✓	✓
BL URL	✓	✓	✓
BL Geo-Protection	✓	✓	✓
Whitelist	✓	✓	✓
Rate Limit			
IP	✓	✗	✓
URL	✓	✗	✓
Geo-Protection	✗	✗	✓
DNS			
DNS Protection	✓	✓	✓
SCORE	**96%**	**73%**	**100%**

CloudFlare Web Challenges coverage is partial.

CloudFlare has a security gap in Rate Limit.

CloudFlare mitigation is good, but F5 and Incapsula mitigation stack is excellent. This allows them to block attacks more accurately.

Figure 4: All-in-All: Mitigation (application protection)

Proxy/Caching

All vendors offer web proxy with caching capabilities. This extremely basic technology is the most effective, and will block many attacks.

However, attackers are persistent today, and can find ways to pass this mitigation, foremost by attacking dynamic pages, leading us to the next most significant mitigation - web challenges.

Web Challenges

Ideally, we want the vendor to address the entire spectrum of challenges. F5 fulfills this demand completely! Incapsula is almost there, with one challenge (NoCAPTCHA ReCAPTCHA) missing. CloudFlare, on the other hand, has more gaps. It does not have the Cookie Validation, which in most cases is all you need to stop an attack with minimal impact on legitimate traffic. CloudFlare does not have Silent Human Investigation and, in case of a JS passing bot, you will be forced to escalate to intrusive NoCAPTCHA ReCAPTCHA. Another disturbing point is that the CloudFlare JS challenge is visible to the user. It informs the user that it is being challenged with an advertisement of CloudFlare at the same time. Not cool.

Signatures

All vendors offer both vendor signatures and user signatures**.** In vendor signatures, CloudFlare has the advantage because it lets you see and even tune them (while Incapsula and F5 signatures perform as a black-box). In user signatures, Incapsula has the upper hand due to the simplicity of signature creation, discussed in the next section.

Rate Limit

CloudFlare does not offer any Rate Limit-based mitigation, which is a significant security gap. Typically, it is not recommended to stop attacks with Rate Limit technologies because it can also “rate limit” legitimate users. However, in some scenarios it is still an important tool. One prominent example is to protect mobile API: Challenges are not efficient, as they often cannot be used with RESTful APIs. In these cases, Rate Limit can be your only savior.

BGP-Based Protection

In addition to Application Protection, also known as Web Protection, all vendors offer Network Protection (BGP-based). All vendors have a black-box approach without any visibility into the technologies being used or the ability to make any configurations.

UX and Reporting

Good User Experience (UX) is more than a nice-to-have feature. It determines how much of the existing functionality you will utilize, how quickly you will understand a security event, and how quickly you can respond while under attack.

	Incapsula	CloudFlare	F5
Look and Feel	Excellent	Good	Basic
Ease of Navigation	Excellent	Excellent	Basic
Deployment			
New website (DNS)	Excellent	Excellent	Basic
New network (BGP)	Full Service	Unknown	Excellent
Security			
Block IP	Excellent	Excellent	Excellent
Block URL	Excellent	Full Service	Good
Web challenge	Excellent	Excellent	Basic
Signatures (vendor)	Blackbox	Excellent	Basic
Signatures (customer)	Excellent	Full Service	Good
Real-Time Reporting			
Real traffic	Excellent	Unknown	Excellent
Blocked traffic	Excellent	Unknown	Excellent
Response time	Excellent	Unknown	Unknown
Events			
Web logs	Excellent	Excellent	Excellent
Email	✓	✗	✓
Call	✓	✓	✓
Syslog	✓	✗	✓
REST	✓	✓	✗
Forensics			
Detailed alert	Excellent	Excellent	Excellent
Event capture file	✗	✗	Good
RT capture file	✗	✗	Full
Score	77%	69%	65%

Incapsula's look and feel is excellent, making the user experience both enjoyable and productive.

Oddly, blocking a URL in CloudFlare can be done only with a request to its support.

CloudFlare is the only one to provide visibility and control of its own signatures.

Incapsula user signatures 'IncapRules' are both powerful and intuitive to use. F5 'iRules' are powerful but less intuitive. CloudFlare signatures are made only by its support.

CloudFlare event methods are partial.

F5 is the only vendor to provide decent forensics by providing capture files (real-time and per event).

Figure 5: All-in-All: UX and Reporting

All vendors provide a decent UX, but undoubtedly Incapsula has a clear lead over the others. Incapsula offers an excellent user interface, navigation, and look and feel. CloudFlare also has a good look and feel, but it still seems a bit outdated compared to today's slick SaaS application designs. F5, on the other hand, is still in the appliance age in terms of UI/UX. Apart from the real-time monitoring part, its interface is outdated and resembles the configuration of an appliance rather than an intuitive cloud application. To summarize: both CloudFlare and Incapsula are easy to navigate. F5 is a little behind.

Deploying Servers

Deploying a new web server is easy with CloudFlare and Incapsula, as well as with F5 Silverline despite its outdated user interface. Deployment of a new network, in contrast, is easiest with Silverline, with which you self-service-wise insert your network and submit it for their NOC for review and final confirmation. With Incapsula, it is full service only – you can add a new network by requesting it from their support.

Configuring Security options

Blocking an IP is easy and simple with all vendors. However, when you want to block a URL, CloudFlare requires that you request it from their support, which seems to be a hassle for such a simple action. The same goes for creating a signature. Incapsula is leading here with its simple yet expressive IncapsRules. F5 offers its famous iRules, which are the most expressive but also more technical. In Customer Signatures, CloudFlare has the upper hand, as its rules are visible and configurable. With Incapsula, you get the rules as black-box.

Real-Time Monitoring (RTM)

F5 and Incapsula monitoring is excellent – granular, doing a good job of showing normal traffic versus attack traffic. With Incapsula it took only 15 seconds for traffic to be displayed, which is very good for a distributed cloud service.

Forensics

With Forensics, F5 has the lead. While all vendors provide informative alerts, F5 allows you to extract the capture of an alert (self-service), and take real-time capture files (full service). Furthermore, the customer can open a chat on an alert and discuss it with the SOC and peers.

Pricing

CloudFlare, Incapsula and F5 do not provide official pricing for their Enterprise service, so you'll have to request a quote.

F5 pricing model is a fully Customer Oriented Pricing Model. The factors that determine the price are: (a) clean traffic rate, (b) number of web sites and data centers and (c) on-demand versus always-on plan. Always-on customers do not pay extra for inclusive managed service, nor do they need to worry about attack data volumes.

Incapsula has a similar pricing model. The only difference is that it also differentiates prices based on traffic volume. This is a disadvantage, as it puts the customer in a difficult spot in terms of making an educated decision about something that cannot really be estimated (see more under Customer Oriented Pricing Model).

The CloudFlare pricing model was unavailable.

SMB Pricing	SMB Pricing is covered in the SMBs – CloudFlare Business vs Incapsula Business section.

Which Solution is Right for You?

Needs-Based Comparison

The DDoS solution you select will depend first and foremost on your security needs and budget. This section includes several comparisons addressing different customer needs and requirements.

The following table will direct you to the right section to read; it shows you the focus points of each category.

Enterprise Web and Infrastructure Protection	Enterprise Web Protection	SMBS
Web Protection Infrastructure protection (network protection) Fully managed services Hybrid protection Price $10K - $50K annually +	Web Protection Web acceleration (CDN) Price $25K - $50K annually +	Web Protection Price $4K annually -

Figure 6: Need-Based Comparison Table

This table can help you focus on which section is relevant for you.

Enterprise Web & Infrastructure Protection - Incapsula Enterprise vs. F5 Silverline

Enterprise Web & Infrastructure Protection is for an enterprise that needs to protect both the website and network assets (VPNs, Class C networks, etc.). Enterprises that look for an end-to-end DDoS solution will require web protection (DNS-based), infrastructure protection (BGP-based), and possibly even an on-premises appliance. The annual budget for a DDoS solution would start at a range of $50K-$100K.

For this report, two vendors provided a 'full-scale enterprise' solution: F5 Silverline and Incapsula. CloudFlare was not included because we did not have sufficient data to determine whether its infrastructure protection is good enough to enter the category.

Deployment & Service Options

	Incapsula Enterprise	F5 Silverline
Diversion Method: DNS		
Always-on	✓	✓
On-demand	✓	✓
Non-web protocols	✓ (IP Protection)	✓ (L4 proxy)
Diversion Method: BGP		
Always-on	✓	✓
On-demand	✓	✓
Service Features		
SSL support – HSM	✗	✗
Emergency response	✓	✓
Fully managed service	✗	✓
Number of data centers	30 see locations	4 San Jose, CA US Ashburn, VA US Frankfurt, DE Singapore, SG

Both vendors support non-web protocols.

F5 offers fully managed service.

Incapsula has 30 data centers, F5 has only 4.

Figure 7: Incapsula vs. F5 - Deployment

The Incapsula Enterprise and F5 Silverline deployment options are very similar. Both offer DNS and BGP-based diversion, a solution for non-web protocols, and On-Demand and Always-On. F5 offers a fully managed service, whereas Incapsula is only partially managed. Although not directly affecting DDoS, Incapsula offers web acceleration and has 30 POPs as opposed to F5, which has only 4 POPs. This can also affect organizations that do not wish to accelerate but to simply maintain their existing latency.

Mitigation

The Web Protection of both vendors is extremely good. They are both fully or almost fully loaded with all the required protection.

The Infrastructure Protection of both F5 and Incapsula is based on a black-box approach, which is less than perfect. Realistically, though, this is the common practice in cloud services.

	Incapsula	F5
Proxy / Caching		
Reverse Proxy	✓	✓
Caching	✓	✓
Web Challenges		
Cookie Validation	✓	✓
JavaScript Challenge	✓	✓
Silent Bot Detection	✓	✓
Modern CAPTCHA	✗	✓
CAPTCHA	✓	✓
Signatures		
Vendor	✓	✓
Customer	✓	✓
Blacklist (BL) / Whitelist		
BL IP	✓	✓
BL URL	✓	✓
BL geo-protection	✓	✓
Whitelist	✓	✓
Rate Limit		
IP	✓	✓
URL	✓	✓
Geo-protection	✗	✓
DNS		
DNS protection	✓	✓
SCORE	96%	100%

Figure 8: Incapsula vs. F5 - Mitigation

F5 is the only one offering the entire web challenge spectrum. types.

Both vendors have excellent mitigation technology coverage.

UX and Reporting

Incapsula has a clear advantage in terms of user experience (UX). F5 Silverline configuration screens seem to have paused in the “network appliance age”, with certain screens of the Cloud WAF service resembling the F5 ASM product.

To balance this picture slightly, F5 Silverline real-time traffic monitoring screens are much better.

When you deploy a new web asset to protect, the UX will be better with Incapsula. However, if you want to protect a new network, with F5 it is self-service and with Incapsula you need full-service.

In forensics, F5 has an advantage, while Incapsula will provide you with the basic alert details. With F5, you can get the event capture file; you can also record the traffic in real time and even instantly open a request for investigation by their SOC.

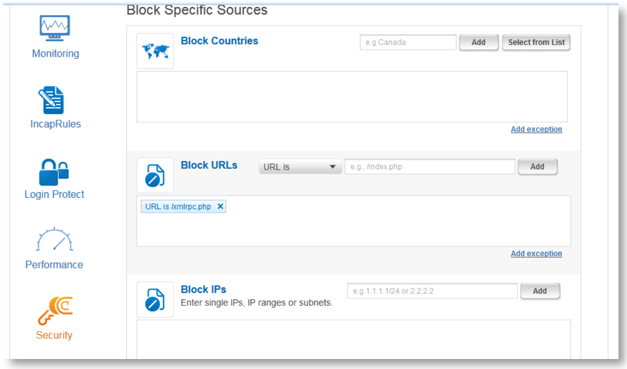
	Incapsula	F5
Look and Feel	Excellent	Basic
Ease of Navigation	Excellent	Basic
Deployment		
New Website (DNS)	Excellent	Basic
New Network (BGP)	Full Service	Excellent
Security		
Block IP	Excellent	Excellent
Block URL	Excellent	Good
Web challenge	Excellent	Basic
Signatures (vendor)	Black-box	Basic
Signatures (customer)	Excellent	Good
Real-Time Reporting		
Real Traffic	Excellent	Excellent
Blocked Traffic	Excellent	Excellent
Response Time	Excellent	Unknown
Events		
Web Logs	Excellent	Excellent
Email	✓	✓
Call	✓	✓
Syslog	✓	✓
REST	~~✓~~	✗
Forensics		
Detailed alert	Excellent	Excellent
Event capture file	✗	Good
RT capture file	✗	Full
Score	77%	65%

Figure 9: Incapsula vs. F5 - UX & Reporting

Incapsula’s look and feel and ease of navigation is much better than F5’s.

Incapsula’s user signatures ‘IncapRules’ is both powerful and intuitive. F5’s ‘iRules’ is powerful but less intuitive.

F5 provides decent forensics with capture files (real-time and per-event).



Block Specific Sources

Block Countries — e.g Canada

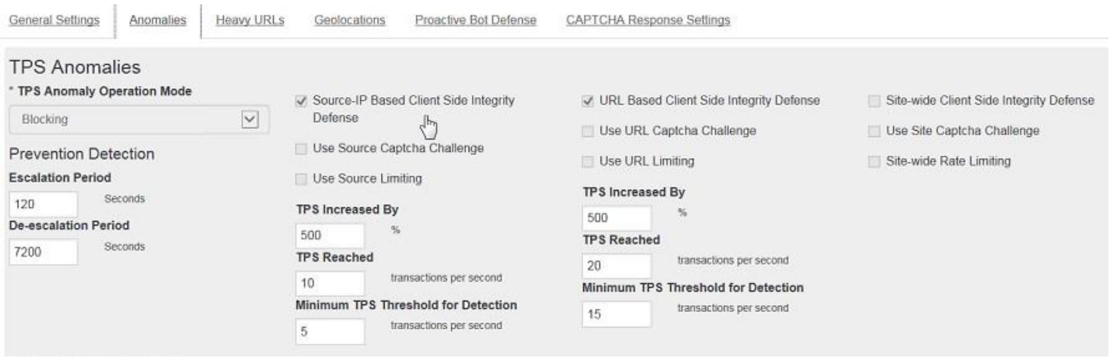
Block URLs — URL is — e.g., /index.php

URL is /xmlrpc.php ✕

Block IPs — e.g 1.1.1.1/24 or 2.2.2.2

Enter single IPs, IP ranges or subnets.

Figure 10: Incapsula vs. F5 - Incapsula Security



TPS Anomalies

* TPS Anomaly Operation Mode: Blocking

Prevention Detection

Escalation Period: 120 Seconds

De-escalation Period: 7200 Seconds

☑ Source-IP Based Client Side Integrity Defense

□ Use Source Captcha Challenge

□ Use Source Limiting

TPS Increased By: 500 %

TPS Reached: 10 transactions per second

Minimum TPS Threshold for Detection: 5 transactions per second

☑ URL Based Client Side Integrity Defense

□ Use URL Captcha Challenge

□ Use URL Limiting

TPS Increased By: 500 %

TPS Reached: 20 transactions per second

Minimum TPS Threshold for Detection: 15 transactions per second

□ Site-wide Client Side Integrity Defense

□ Use Site Captcha Challenge

□ Site-wide Rate Limiting

Figure 11: An F5 Security Configuration Screen

Pricing

Both vendors do not publicly provide their enterprise plans. Their pricing factors are relatively similar. The only difference is that Incapsula also adds attack traffic as a pricing factor, which we consider a disadvantage (see Customer Oriented Pricing Model).

Bottom Line

The technical comparison of the two vendors shows that there is no clear-cut conclusion. Both vendors offer rich deployment and mitigation options.

Enterprises looking for a fully managed service will find a better home with F5. The user interface of Incapsula is clearly better, and this is not a luxury item anymore.

Another factor that may be relevant in your decision is that Incapsula offers a CDN, while F5 Silverline does not. This can be a critical advantage if you need the data center to be in specific geographical areas either due to regulation or to reduce latency.

How to make a decision?	• Receive a quote. • Investigate the stability and support of each vendor. • Read the How to Complete the Vendor Selection section.

Enterprise Web Protection - CloudFlare Enterprise vs. Incapsula Enterprise

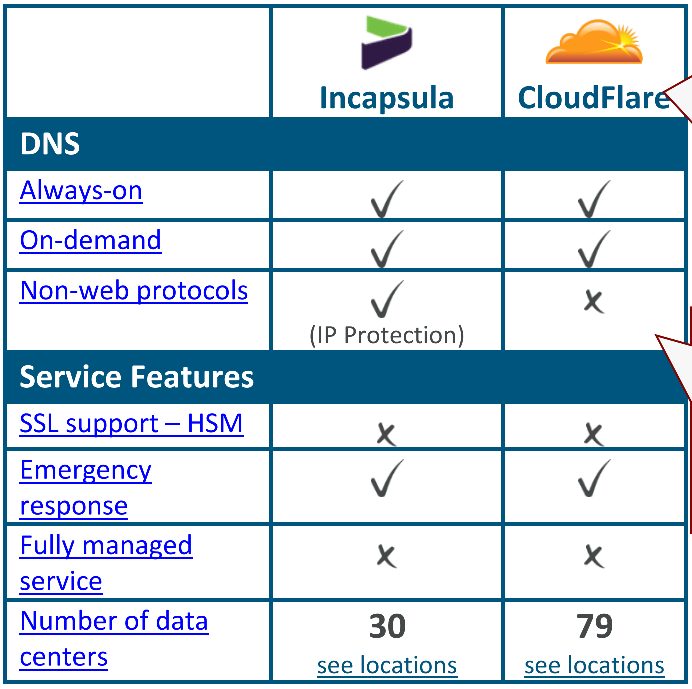
Some organizations require strong web protection (DNS diversion), but can do without infrastructure protection (BGP diversion) or a physical appliance. This will be the case when the DDoS threat and/or the potential damage are not considered critical enough to justify the extra investment.

For such requirements, CloudFlare and Incapsula provide solutions that also include acceleration built into the DDoS service.

Deployment & Service Options

With a cloud-based service, both CloudFlare and Incpasula offer basic web protection (DNS) and network protection (BGP). They both provide free tiered services, as well as services for SMBs and for Enterprises.

CloudFlare offers 86 POPs as opposed to Incapsula, with only 30. However, the effect of this on DDoS mitigation is only indirect (see Number of Data Centers).



	Incapsula	CloudFlare
DNS		
Always-on	✓	✓
On-demand	✓	✓
Non-web protocols	✓ (IP Protection)	✗
Service Features		
SSL support – HSM	✗	✗
Emergency response	✓	✓
Fully managed service	✗	✗
Number of data centers	30 see locations	79 see locations

Figure 12: Incapsula vs. CloudFlare - Deployment

On the cloud front, vendor deployment and service options are relatively similar.

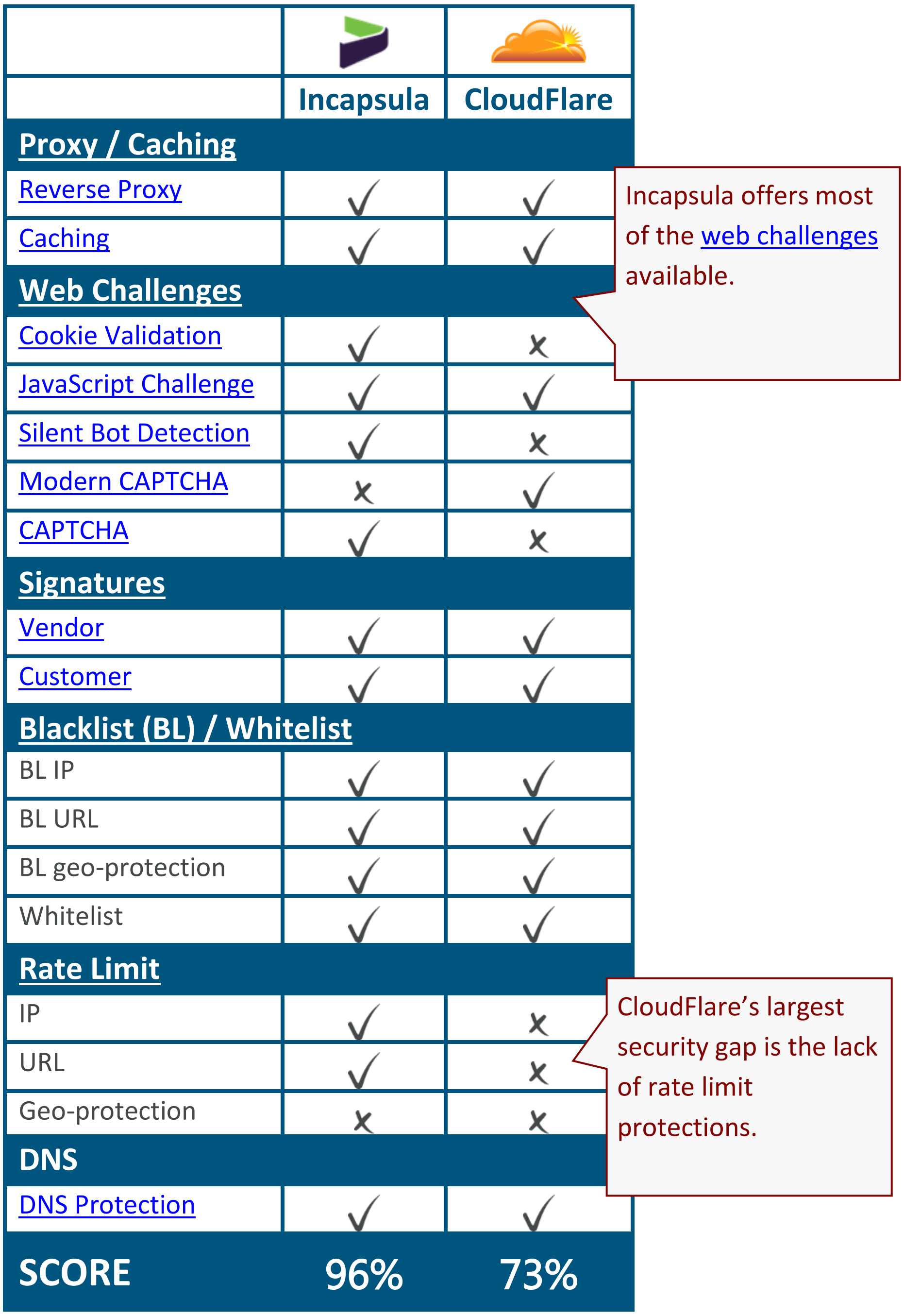
Incapsula can protect non-web protocols even if you don't have a class C network.

If your organization has a non-web service like a proprietary protocol, only Incapsula can serve you with its latest IP Protection topology.

Mitigation

Web Proxy and Caching

Both vendors have web proxy with caching capabilities. This may not be the most sophisticated technology, yet it is the most effective and will succeed in blocking many attacks. However, today's attackers are persistent and will find ways to bypass this mitigation, primarily by attacking dynamic pages.



	Incapsula	CloudFlare
Proxy / Caching		
Reverse Proxy	✓	✓
Caching	✓	✓
Web Challenges		
Cookie Validation	✓	✗
JavaScript Challenge	✓	✓
Silent Bot Detection	✓	✗
Modern CAPTCHA	✗	✓
CAPTCHA	✓	✗
Signatures		
Vendor	✓	✓
Customer	✓	✓
Blacklist (BL) / Whitelist		
BL IP	✓	✓
BL URL	✓	✓
BL geo-protection	✓	✓
Whitelist	✓	✓
Rate Limit		
IP	✓	✗
URL	✓	✗
Geo-protection	✗	✗
DNS		
DNS Protection	✓	✓
SCORE	**96%**	**73%**

Incapsula offers most of the web challenges available.

CloudFlare's largest security gap is the lack of rate limit protections.

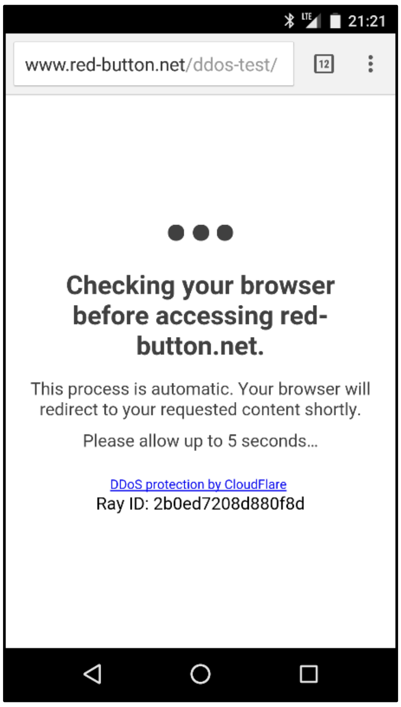
Figure 13: Incapsula vs. CloudFlare - Mitigation

Web Challenges

This leads us to the next most significant mitigation - web challenges. Ideally, we want the vendor to provide the entirety of the challenge spectrum (read more). Incapsula offers four out of the five challenges. The only one missing is the modern CAPTCHA; in the unlikely event that its JS challenge will not be effective, it would have been slightly better to have this. CloudFlare offers only two out of the five challenges. It is not that CloudFlare will not be able to stop DDoS attacks; it is simply that you will need to use a bigger hammer than you intended. CloudFlare does not have plain Cookie Validation, and in most cases this will be enough to stop the attack with minimal impact to legitimate users and legitimate bots. CloudFlare also does not have Silent Human Investigation and, in the case of a JS passing bot (e.g., PhantomJS), you will be forced to escalate to the intrusive modern CAPTCHA. The traditional CAPTCHA is also not used by CloudFlare, but because it has the modern version, this is reasonable. Another annoying aspect is that the CloudFlare JS challenge is visible to the user.

Signatures

Both vendors offer signature and customer signature options. CloudFlare is better at the vendor signature, as it provides visibility to the signature name and allows the user to control its action, while with Incapsula it is a black-box service. In user signatures, Incapsula is better, with its excellent pre-IncapRules language, allowing even beginners to compose meaningful signatures. CloudFlare takes a different approach; you write in plain English what you want the signature to do and submit it. CloudFlare’s support writes the signature for you, which means you will not be able to review it or change its action.



Checking your browser before accessing red-button.net.

This process is automatic. Your browser will redirect to your requested content shortly.

Please allow up to 5 seconds…

DDoS protection by CloudFlare
Ray ID: 2b0ed7208d880f8d

Figure 14: CloudFlare Web Challenge
CloudFlare’s visible and intrusive challenge. The intention here is not clear, but it acts as an advertisement for CloudFlare at the expense of its customer UX.

Rate Limit

In terms of Rate Limit, CloudFlare has a large and important gap. While usually it is not recommended to stop attacks with Rate Limit technologies that eventually can also “rate-limit” legitimate users, in some scenarios, such as to protect mobile APIs, it is still important. Challenges are not good, as they often cannot be used with RESTful API, and Rate Limit can be your only savior.

Network Protection

Incapsula Network Protection (BGP) is a black-box. You cannot configure or understand what actions are taking place and how effective they are. No information could be received from CloudFlare on this issue.

UX and Reporting

User Experience (UX) is important, as it determines how much of the existing functionality you will utilize, how quickly you will understand a security event, and how quickly you can respond while under attack.

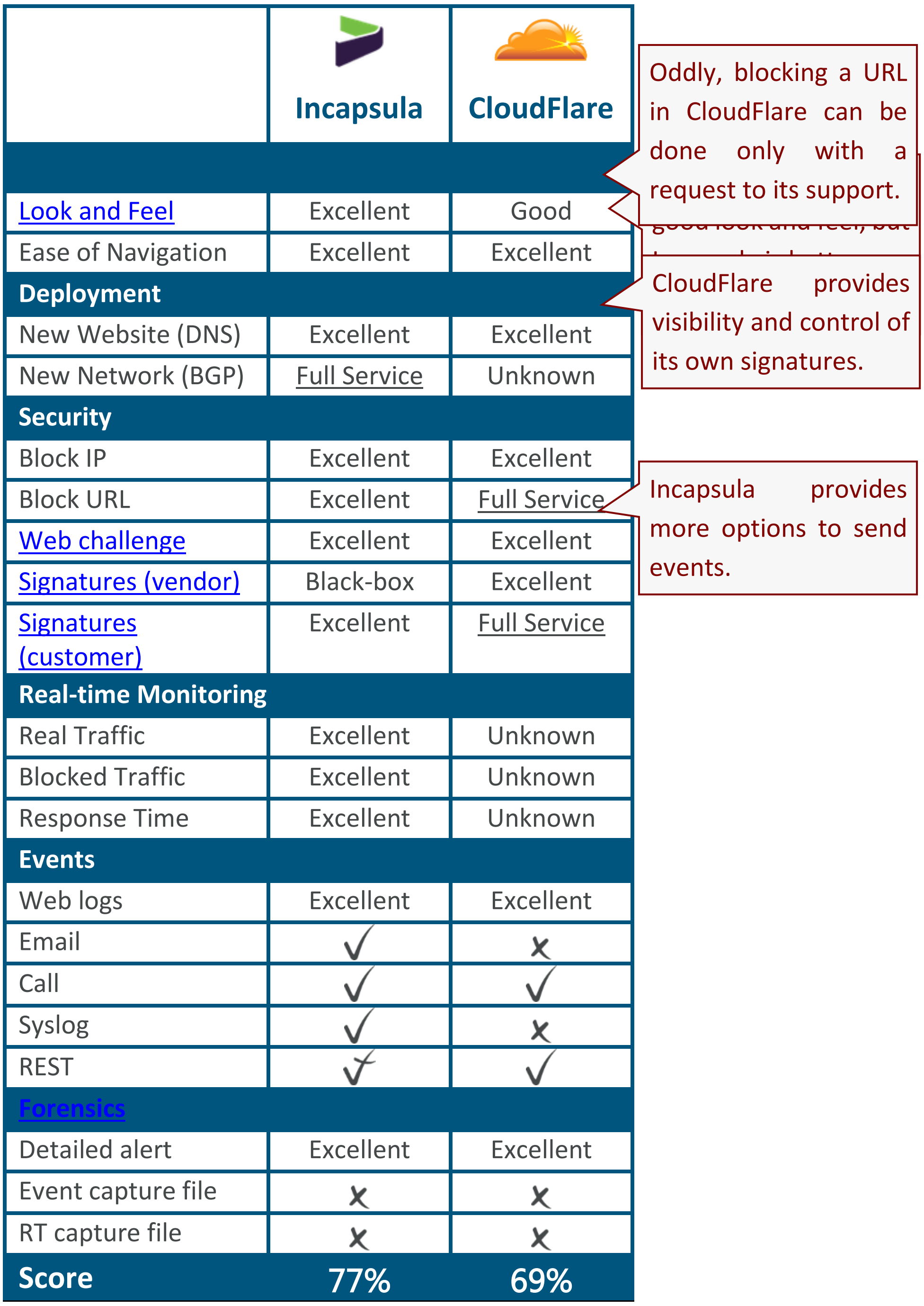
In UX, per se, the difference between vendors is not dramatic. Incapsula's look and feel is excellent, while CloudFlare is somewhat old-school relative to cloud services. Nevertheless, it is still very easy to navigate and find the function you need with both vendors.

Security Configuration

Both vendors' security configuration is good, and the limitation of each vendor in terms of using signatures has been covered earlier. One disturbing element with CloudFlare is the ability to independently block a URL – probably the most basic thing you can ask from a WAF. This can be done, but it is a full-service feature. Why not provide a simple interface just like the one provided for blocking an IP or a country?

Real-Time Monitoring

We did not have access to CloudFlare's real-time monitoring (RTM). Incapsula's RTM, which we did review, is great. It is granular and does a good job of showing allowed versus blocked traffic. It took about 15 seconds for traffic to appear, which is excellent performance for a cloud service with distributed POPs.



	Incapsula	CloudFlare
Look and Feel	Excellent	Good
Ease of Navigation	Excellent	Excellent
Deployment		
New Website (DNS)	Excellent	Excellent
New Network (BGP)	Full Service	Unknown
Security		
Block IP	Excellent	Excellent
Block URL	Excellent	Full Service
Web challenge	Excellent	Excellent
Signatures (vendor)	Black-box	Excellent
Signatures (customer)	Excellent	Full Service
Real-time Monitoring		
Real Traffic	Excellent	Unknown
Blocked Traffic	Excellent	Unknown
Response Time	Excellent	Unknown
Events		
Web logs	Excellent	Excellent
Email	✓	✗
Call	✓	✓
Syslog	✓	✗
REST	✓	✓
Forensics		
Detailed alert	Excellent	Excellent
Event capture file	✗	✗
RT capture file	✗	✗
Score	77%	69%

Oddly, blocking a URL in CloudFlare can be done only with a request to its support.

good look and feel, but

CloudFlare provides visibility and control of its own signatures.

Incapsula provides more options to send events.

Figure 15: CloudFlare vs. Incapsula - UX & Reporting

You can consume the security events generated by Incapsula in several ways - on its portal, by receiving an email, or via a syslog. When under attack, it will also call you. CloudFlare displays events on its portal and will call you in case of a severe attack. It lacks a push notification method and offers no email or syslog options. CloudFlare does offer a REST API to pull the alerts, but it is unlikely that everyone would like to implement a REST client to know what is going on with their network.

Forensics

With Forensics, both vendors offer the same basic level. You will get a detailed alert, but you cannot see a capture file associated with an alert or take a capture file in real time.

Pricing

CloudFlare and Incapsula, like most vendors, do not provide official pricing for their Enterprise service; the only way to retrieve this information is to request a quote.

SMB Pricing	SMB Pricing is covered in the SMBs – CloudFlare Business vs. Incapsula Business section.

Bottom Line

If we are taking the liberty to compare the vendors from a higher ground, observing the entire portfolio, it seems that CloudFlare targets a much wider audience. It offers numerous services, operates in an application market, and appeals to the multiple needs of different organizations, especially SMBs. Incapsula offers fewer services, but they seem to be more complete and focused.

From the narrow DDoS point of view, both services are mature; choosing either of them to protect your service from DDoS attacks would be a good option. However, Incapsula's service is more complete than CloudFlare's in all the categories reviewed. Put differently, if you need only DDoS protection and you receive the same quote, Incapsula has a clear advantage.

How to make a decision?	• Receive a quote. • Investigate the stability and support of each vendor. • Read the How to Complete the Vendor Selection section.

SMBs – CloudFlare Business vs. Incapsula Business

Not everyone needs a full-blown enterprise DDoS solution. If you cannot spend more than $5,000 an year on DDoS and you have limited DDoS concerns, an SMB type of solution offered by Incapsula Enterprise and F5 Silverline may be suitable for your needs.

What Type of DDoS Services are Offered to SMBs?

CloudFlare Business and Incapsula Business are intended for SMBs and for enterprises with very modest DDoS needs. The Business plan is a subset of the Enterprise plan, so you'll get approximately only 30% of the DDoS functionality, so to speak (but pay a fraction of the cost).

The Subset of Services Business Plans Receive	
Web Protection	✓
Infrastructure Protection	✗
DDoS mitigation	✓
Security logs	✓
Real-time reporting	✗
Phone support	✗
Emergency response	✓✗

Figure 16: Services That are Lost and Remain in the BUSINESS Plans (for SMBs)

Deployment

The comparison table of SMBs is much simpler than those of the Enterprise plan. The reason for this is that most options are not available for SMBs. In this context, there is no difference between the two vendors.

	Incapsula	CloudFlare
DNS		
Always-on	✓	✓
On-demand	✓	✓
Service Features		
Number of data centers	30 see locations	79 see locations

Figure 17: Incapsula Business vs. CloudFlare Business - Deployment

Mitigation

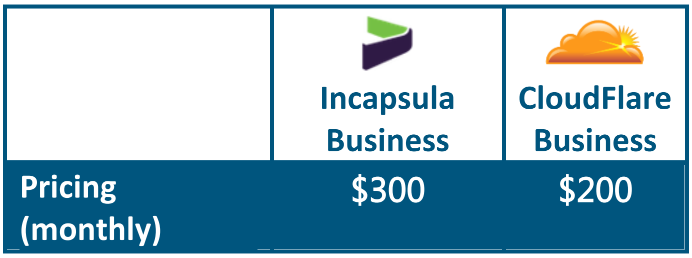
The mitigation options are very similar to the Enterprise plan. Read the Enterprises' Mitigation comparison to learn about the differences. The bottom line is that while both vendors can stop DDoS attacks, Incapsula has a clear advantage.

UX and Reporting

The User Experience (UX) of the Business plan is very similar to that of the Enterprise plan. Read the Enterprises' UX and Reporting comparison to learn about the differences. Both vendors are good, but Incapsula has an advantage.

Pricing

Incapsula’s monthly fee for the Business service is $300 USD vs. $200 charged by CloudFlare. Note that these prices are for a single web site.



	Incapsula Business	CloudFlare Business
Pricing (monthly)	$300	$200

Figure 18: Business Plan Pricing

Bottom Line

Incapsuala’s advantage over CloudFlare as presented in the enterprise solution segment is less significant when discussing SMBs (because many features in which it has an advantage are not available). Still, the Incapsula advantage remains; it offers more tools to fight DDoS attacks as well as more challenges, and allows you to compose rules yourself rather than wait for support. It also offers rate limit options, which can be very important if you need to protect RESTful APIs.

On the other hand, organizations may have non-DDoS considerations and decide that CloudFlare is better or has an appealing application that Incapsula does not offer. Such considerations are naturally not part of this report. Another factor is the cheaper price offered by CloudFlare.

Another point in favor of Incapsula is future growth. An enterprise plan may become relevant for an SMB down the road due to growth or an increased threat level, in which case Incapsula’s DDoS mitigation is a more secure investment.

Individual Vendor Review

Imperva Incapsula

Imperva Incapsula DDoS Product Line

Incapsula is a company founded by Imperva in 2009. It spun off on its own for a short while, but was then re-acquired by Imperva in 2014. Incapsula started as a cloud-based WAF, but like many similar services became a CDN+WAF+DDOS cloud solution. It served SMB originally, but with time its DDoS appetite increased and it started to compete at the enterprises level. Because of this, it had to complete its BGP-based offering (on top of its traditional ion method). This latest addition was followed by a unique IP Protection diversion method fully released in 2016. With its acquisition by Imperva, the joined brand has Imperva WAFs, which also has on-premises DDoS capabilities. Together, the vendor has hybrid protection and the portfolio is very mature.

The following 'Deployment' section analyzes the Incapsula service and Imperva WAF product, while the rest of the analysis focuses on the Incapsula cloud service.

Incapsula Enterprise

Deployment & Service Options

On the cloud front, Incapsula supports all diversion methods, including DNS and BGP, and has introduced a new diversion method - IP Protection - to the market (read more). The significance of supporting all diversion methods must be emphasized; the Incapsula service can be shaped to support any organization, but more important is the fact that it reduces risks. If the organization migrates some of its services to the cloud, acquires a Class C network, forfeits a Class C, or undergoes any other architectural change, Incapsula will still be able to follow and provision the new architecture.

On the on-premises front, Imperva offers both a physical and virtual WAF. The company, however, does not offer a dedicated DDoS appliance.

Imperva-Incapsula has two deployment limitations. The first is that it does not have a DDoS-dedicated appliance. Organizations that wish to invest in very strong on-premises DDoS protection are likely to avoid Incapsula. The second limitation is that it does not have a fully managed service, although a partially managed service can be added on top of its Enterprise plan.

	Incapsula
Diversion Method: DNS	
Always-on	✓
On-demand	✓
Non-web protocols	✓ (IP Protection)
Diversion Method: BGP	
Always-on	✓
On-demand	✓
Service Features	
SSL support – HSM	✗
Emergency response	✓
Fully managed service	✗
Number of data centers	**30** see locations
Entry Level	
SMB plans	✓

Figure 19: Imperva-Incapsula Deployment

Incapsula's deployment and service options cater to most organizations. Imperva also has a WAF appliance.

Incapsula's unique 'IP Protection' can protect non-web services even if the organization does not have a class C network.

The Incapsula service is partially managed, but is not a fully managed service.

SMBs and enterprises with modest budgets have a lower entry level.

Mitigation

Application Protection

Incapsula Web Protection is fully loaded with mitigation technology and is almost complete (96%). The wide technology coverage combined means that virtually all type of attacks can be blocked, and can be blocked accurately (with minimal significant false positives).

Infrastructure Protection

The network mitigation is a black-box, so that the customer cannot assess the quality of the protection nor control it.

	Incapsula
Proxy / Caching	
Reverse Proxy	✓
Caching	✓
Web Challenges	
Cookie Validation	✓
JavaScript Challenge	✓
Silent Bot Detection	✓
Modern CAPTCHA	✗
CAPTCHA	✓
Signatures	
Vendor	✓
Customer	✓
Blacklist (BL) / Whitelist	
BL IP	✓
BL URL	✓
BL geo-protection	✓
Whitelist	✓
Rate Limit	
IP	✓
URL	✓
Geo-protection	✗
DNS	
DNS Protection	✓
SCORE	**96%**

Figure 20: Incapsula Mitigation

Incapsula offers almost all the web challenges in the spectrum.

Incapsula mitigation technologies are very complete.

UX & Reporting

	Incapsula
Look and Feel	Excellent
Ease of Navigation	Excellent
Deployment	
New Website (DNS)	Excellent
New Network (BGP)	Full Service
Security	
Block IP	Excellent
Block URL	Excellent
Web challenge	Excellent
Signatures (vendor)	Blackbox
Signatures (customer)	Excellent
Security	
Real Traffic	Excellent
Blocked Traffic	Excellent
Response Time	Excellent
Events	
Web Logs	Excellent
Email	✓
Call	✓
Syslog	✓
REST	✓
Forensics	
Detailed Alert	Excellent
Event Capture File	✗
RT Capture File	✗
Score	**77%**

Figure 21: Incapsula - UX & Reporting

Incapsula's look and feel is excellent, making the user experience both enjoyable and productive.

Incapsula's vendor signatures cannot be viewed or configured.

Incapsula's user signatures 'IncapRules' are both powerful and intuitive to use.

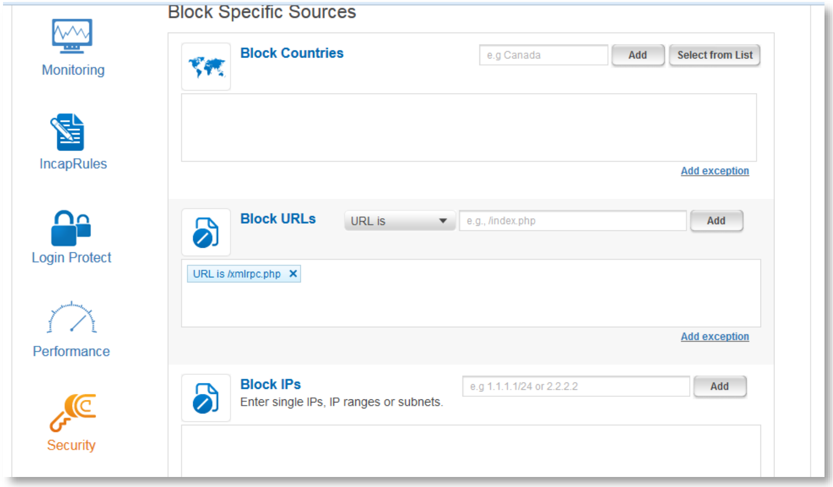
Multiple methods to receive alerts.

Detailed alerts, but capture files cannot be extracted.

Configuration

Incapsula’s user experience (UX) is at the top level of a modern SaaS service. Both beginners and experts will find it efficient.

Incapsula offers other services (CDN, WAF, LB). The downside of this is that there is no single DDoS view on the system and DDoS features are spread over two or three locations. Overall, this is a minor issue.



Block Specific Sources

Block Countries: e.g Canada

Block URLs: URL is ▾ e.g. /index.php

URL is /xmlrpc.php ✕

Block IPs: Enter single IPs, IP ranges or subnets. e.g 1.1.1.1/24 or 2.2.2.2

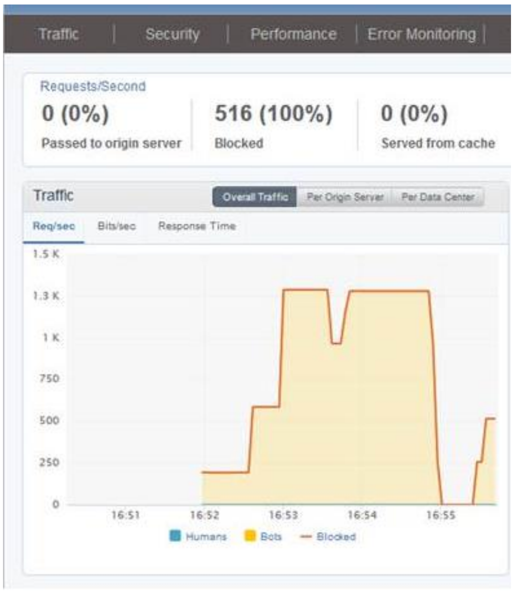
Figure 22: Incapsula User Interface

Incapsula has a moderns SaaS UX. It is very easy to master and allows both beginners and experts to utilize it efficiently.

The User Signatures, called 'IncapRules', use a very intuitive language, allowing even beginners to compose complex signatures including rate-limit rules. Nevertheless, this language does have limitations, and not everything you wish can be expressed. In this case, Incapsula’s professional support team can be used to compose such rules.

Real-Time Monitoring

Incapsula provides sufficient real-time monitoring (RTM) that is especially valuable while under attacks. The RTM graph is very granular, clearly showing allowed traffic in comparison to blocked traffic, and the response time is excellent. It takes only 15 seconds for the traffic to appear, which is very good for a distributed cloud service.



Requests/Second

0 (0%) Passed to origin server

516 (100%) Blocked

0 (0%) Served from cache

Figure 23: Real-Time Reporting

Incapsula provides sufficient real-time reporting that is especially good for monitoring attacks and mitigation.

WORTH NOTING

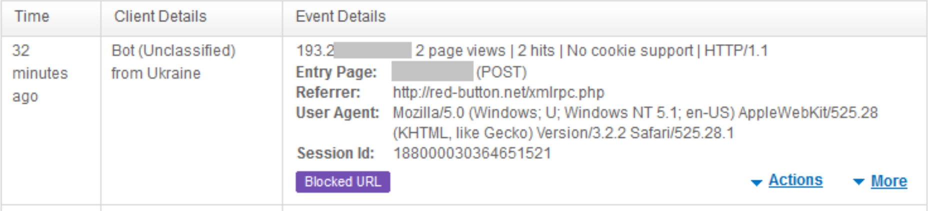
Incapsula User Interface Standard

Driving Incapsula is like driving a spaceship. It starts with a comfortable feeling by just gazing at the screen. It continues with the navigation process, which is very intuitive. For example, it is very easy to find the location of a certain property you configured a month ago. Real-time reporting is immediate and flexible. The IncapRules presentation and syntax allow a novice user to create expert signatures. This intuitive UI increases productivity and improves security, and can shorten mitigation time when under real-time attacks.

Reporting

Incapsula provides multiple reporting methods:

- Email
- Syslog
- Call from Incapsula support



Time	Client Details	Event Details
32 minutes ago	Bot (Unclassified) from Ukraine	193.2[redacted] 2 page views | 2 hits | No cookie support | HTTP/1.1 **Entry Page:** [redacted] (POST) **Referrer:** http://red-button.net/xmlrpc.php **User Agent:** Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/525.28 (KHTML, like Gecko) Version/3.2.2 Safari/525.28.1 **Session Id:** 188000030364651521 Blocked URL

Figure 24: Incapsula Alerts
Incapsula alerts are very accessible and detailed. It is a WAF-like reporting, including HTTP headers.

Incapsula does support REST API for a multitude of its functions, but not for security events, as it has the Syslog option to compensate for that.

DDoS Forensic

Incapsula's DDoS Forensic is comprised of detailed and very accessible alerts. It offers a multitude of other real-time and historical reports that are not covered here, some of which can be used for DDoS.

An important caveat is that there are no logs for Infra. Protection at all, and there is no ability to extract a capture file.

Forensic Function	Exist
Detailed alert	✓
Real-time capture file	✗
Historical capture file	✗

Figure 25: Incapsula Forensics
Incapsula provides detailed alert s,

Pricing

Incapsula, like most vendors, does not publish its Enterprise pricelist, so the only way to know it is to request a quote.

Price Model

Incapsula's pricing model is not a fully Customer-Oriented Pricing Model. We don't like the fact that the pricing factor is based on the 'maximal attack size' because it rolls to the customer a responsibility that is difficult to address.

Pricing Factors
Always-on / On-demand
Clean traffic
Number of websites and data centers
Maximal attack size

Figure 26: Incapsula Pricing Model

Incapsula Business (for SMB)

Incapsula's Business plan costs $300 monthly ($3,600 USD annually) per web site, and gives you DDoS protection with some important limitations: no phone support, no real-time monitoring, and no network protection (BGP). Despite these limitations, it provides a good DDoS entry point for organizations with clear DDoS needs but without the budget for full-fledged protection.

F5

F5 Networks (in short, 'F5') was founded in 1996 and is known for its load-balancing products. In 2004 it acquired and incorporated a WAF technology branded as ASM (Application Security Manager). When DDoS became mainstream, it added to the WAF multiple DDoS mitigation features.

In 2014 it acquired Defense.Net, a cloud-based DDoS mitigation service similar to Prolexic. (In fact, it is a reboot of the same founder.) Defense.Net was branded as F5 Silverline. With this step, F5 positioned itself as a significant player in the DDoS market, at least based on its technology portfolio.

F5 Silverline

Deployment & Service Options

F5 Silverline's cloud-based protection provides both BGP and DNS-based diversion, always-on and on-demand, and supports L4 proxy for non-web protocols.

For an on-premise solution, F5 has its matured WAF ASM, which can reside on top of its BIG IP load-balancer or stand alone. It can be either physical or virtual.

F5 easily addresses the deployment requirements of most enterprise organizations. It will also secure the investment for those organizations, as it offers various means to expand the service, especially by adding a hybrid solution.

F5 has two main deployment limitations. The first is that it does not have a dedicated DDoS Appliance for organizations that wish to protect most attacks on-site rather than on the cloud. The second limitation is that F5 Silverline has no offering for SMBs or enterprises with modest DDoS needs. Its cheapest cloud service is $75,600 USD per year (pricelist). F5's solutions can be very appealing to organizations that already have the common F5 BIG IP.

	F5
DNS	
Always-on	✓
On-demand	✓
Non-web protocols	✓ (L4 proxy)
BGP	
Always-on	✓
On-demand	✓
Service Features	
SSL support – HSM	x
Emergency response	✓
Fully managed service	✓
Number of data centers	4 San Jose, CA US Ashburn, VA US Frankfurt, DE Singapore, SG
Entry Level	
SMB plans	x

Figure 27: F5 Deployment & Service Options

F5 deployment and service options can cater to most organizations. F5 also has a WAF appliance.

F5's unique 'L4 Proxy' can protect non-web services even if the organization does not have a class C

F5 offers fully managed services.

F5's entry level does not allow SMBs to join in.

F5 Silverline has four data centers, which is very limited. (In comparison, Incapsula has 30, CloudFlare 86, and Akamai 1000.) However, F5 Silverline is not intended to act as a CDN, and this is not considered a direct limitation from a mere DDoS point of view. It can be a drawback to customers who have specific latency or data center location requirements (see Number of Data Centers).

Mitigation

Web Protection

F5 has literally all the mitigation technologies mapped by this report (100% coverage). Most are accessible directly, and the rest can be configured via its iRules. The perfect coverage allows F5 to not only protect virtually any attack out there, but to protect it very accurately (without false positive).

Infrastructure Protection

F5's Silverline Route is its network protection, based on BGP diversion. Like all cloud-based services reviewed in this report, the network mitigation is a black-box, which does not enable assessing the quality of protection. On the bright side, F5 Silverline is forthcoming with its data center architecture, and the details provided provide certain, yet limited, confidence. See more details below.

	F5
Proxy / Caching	
Reverse Proxy	✓
Caching	✓
Web Challenges	
Cookie Validation	✓
JavaScript Challenge	✓
Silent Bot Detection	✓
Modern CAPTCHA	✓
CAPTCHA	✓
Signatures	
Vendor	✓
Customer	✓
Blacklist (BL) / Whitelist	
BL IP	✓
BL URL	✓
BL geo-protection	✓
Whitelist	✓
Rate Limit	
IP	✓
URL	✓
Geo-protection	✓
DNS	
DNS Protection	✓
SCORE	**100%**

Figure 28: F5 Mitigation

F5 offers all the web challenges in the spectrum.

F5 mitigation technologies are literally complete.

Data Center Structure

F5 Silverline is forthcoming with its data center structure and states its general structure, providing visibility to its customers and prospects.

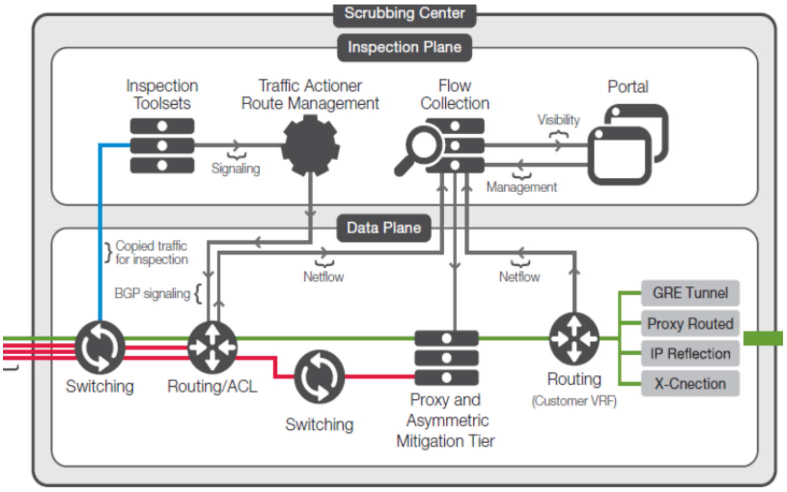


Figure 29: F5 Scrubbing Center Architecture

F5 Silverline scrubbing center structure. F5's forthcoming approach allows customers a better understanding. It is considered a great value for the customer.

WORTH NOTING

Scrubbing Center White-Box Approach

Vendors specify the number of scrubbing centers (SCs) and locations, but the scrubbing centers themselves are presented as black-boxes. F5 Silverline is unique in specifying its SC architecture. This report gives credit to such an approach because it benefits end users. It allows for scrutiny and criticism; for example, if any of the technologies used has limitations, customers can inquire how they will be affected.

Many vendors hesitate to reveal their architecture due to competition; however, the white-box approach benefits the end user and is therefore encouraged.

UX and Reporting

Configuration

The experience with the F5 user interface starts with deployment options. The screens are very basic, yet efficient. When you configure a new entry and save it, the input goes to the SOC, which then approves and applies the setting. This adds a layer of expert control without affecting the positive self-service approach.

The mitigation screens of the F5 Silverline are very similar to those of the F5 ASM (as, indeed, the former is based upon the latter). The screens are not very well organized - there are too many objects and it is difficult to distinguish between the detection and mitigation parameters. It feels more like a traditional network appliance UI than a modern, cloud-based service.

	F5
Look and Feel	Basic
Ease of Navigation	Basic
Deployment	
New Website (DNS)	Basic
New Network (BGP)	Excellent
Security	
Block IP	Excellent
Block URL	Good
Web challenge	Basic
Signatures (vendor)	Basic
Signatures (customer)	Good
Security	
Real Traffic	Excellent
Blocked Traffic	Excellent
Response Time	Unknown
Events	
Web Logs	Excellent
Email	✓
Call	✓
Syslog	✓
REST	✗
Forensics	
Detailed Alert	Excellent
Event Capture File	Good
RT Capture File	Full
Score	65%

F5's look and feel and navigation are only basic.

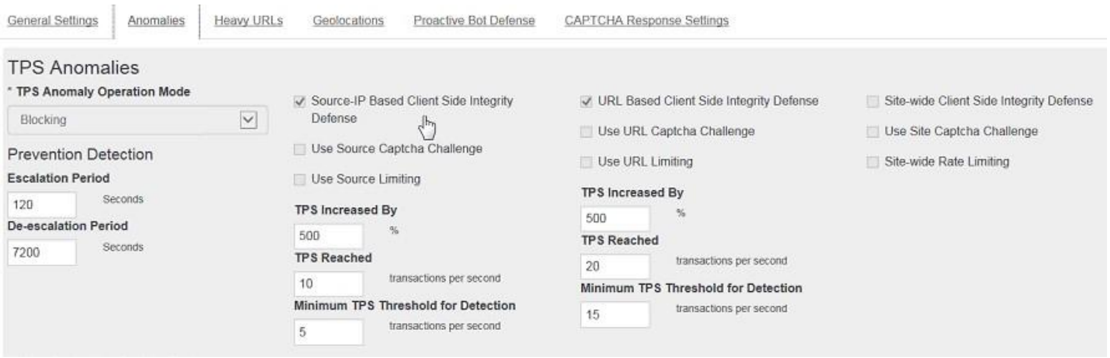
F5's vendor signatures are not available to view or configure.

F5 users can create signatures using the iRule syntax.

Multiple methods to receive alerts.

Excellent forensics with good alerts and the ability to extract capture files.

Figure 30: F5 - UX & Reporting



General Settings | Anomalies | Heavy URLs | Geolocations | Proactive Bot Defense | CAPTCHA Response Settings

TPS Anomalies

* TPS Anomaly Operation Mode

Blocking

Prevention Detection

Escalation Period

120 Seconds

De-escalation Period

7200 Seconds

☑ Source-IP Based Client Side Integrity Defense

□ Use Source Captcha Challenge

□ Use Source Limiting

TPS Increased By

500 %

TPS Reached

10 transactions per second

Minimum TPS Threshold for Detection

5 transactions per second

☑ URL Based Client Side Integrity Defense

□ Use URL Captcha Challenge

□ Use URL Limiting

TPS Increased By

500 %

TPS Reached

20 transactions per second

Minimum TPS Threshold for Detection

15 transactions per second

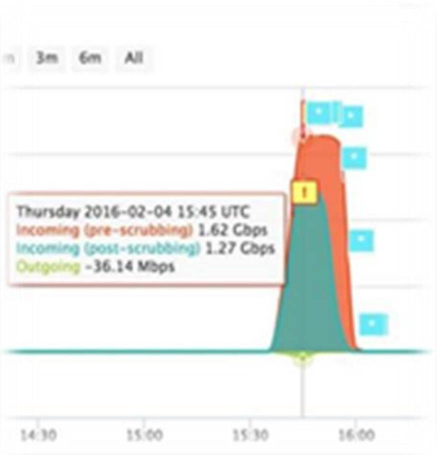
□ Site-wide Client Side Integrity Defense

□ Use Site Captcha Challenge

□ Site-wide Rate Limiting

Figure 32: Mitigation Configuration

An abundance of configuration options that are not well-organized makes it difficult to distinguish between detection and mitigation properties.



Thursday 2016-02-04 15:45 UTC
Incoming (pre-scrubbing) 1.62 Gbps
Incoming (post-scrubbing) 1.27 Gbps
Outgoing -36.14 Mbps

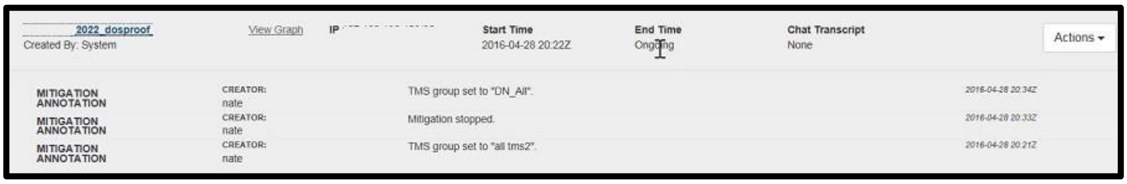
Real-Time Monitoring

Things get better in terms of real-time reporting. As you can see in the snapshots, the graphs are nice and accurate.

Figure 31: F5 Real-Time Monitoring

DDoS Forensic

The logs of the network protection and application protection are unified. There is an interesting chat feature allowing you to issue a query to the SOC team to get more details about a security log. This is an excellent "SOC management tool" indicating the highly managed service level that F5 provides.



[redacted]2022_dosproof
Created By: System

View Graph

IP [redacted]

Start Time
2016-04-28 20:22Z

End Time
Ongoing

Chat Transcript
None

MITIGATION ANNOTATION	CREATOR: nate	TMS group set to "DN_All".	2016-04-28 20:34Z
MITIGATION ANNOTATION	CREATOR: nate	Mitigation stopped.	2016-04-28 20:33Z
MITIGATION ANNOTATION	CREATOR: nate	TMS group set to "all tms2".	2016-04-28 20:21Z

Figure 33: F5 Silverline Security Logs

A live 'chat' allows you to issue a query to investigate or clarify a log with support.

Pricing

F5 Silverline has a fully Customer-Oriented Pricing Model. It is based on three parameters. The first is the service type: always-on versus on-demand ("always available" in F5's language). The second is the clean traffic bandwidth, and the third is the DC size and number of VIPs combined into one parameter.

F5 Silverline does not charge extra for its fully managed service, but realistically only always-on will benefit from it. It does not charge for attack traffic bandwidth; this is a unique yet very important positive factor in terms of its pricing model.

Pricing Factors
Always-on / On-demand
Clean traffic
Number of websites and data centers

Figure 34: F5 Pricing Model

CloudFlare

DISCLAIMER	**No vendor feedback on presented data** The vendor did not respond to the research; therefore, there is some missing data and information may be inaccurate.

Overview

CloudFlare's motto is "we will supercharge your website". Its service includes CDN, Web Application Firewall (WAF), DDoS mitigation, analytics, and optimization, and it has an application market with 25 providers at last count. Having said that, this report has a single objective - DDoS, and CloudFlare is reviewed here for its DDoS mitigation traits only.

CloudFlare Enterprise

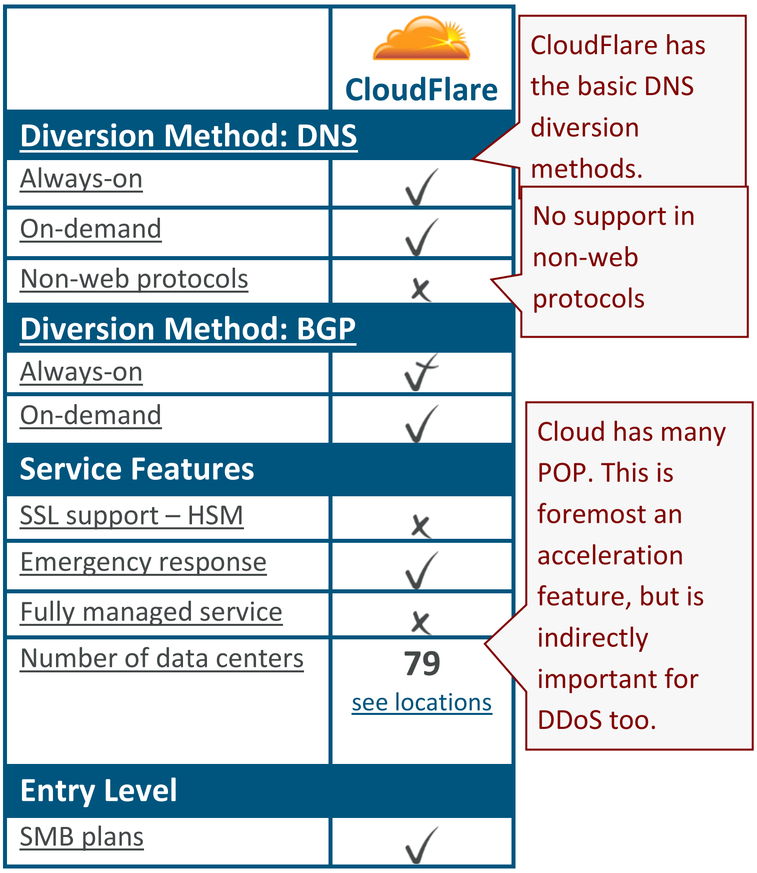
Deployment & Service Options

CloudFlare's main deployment is based on DNS diversion (Web Protection). BGP is also available to protect the origin IP, but we did not find sufficient details about the extent of its always-on option.

CloudFlare has only cloud services, with no on-premises appliance or virtual appliances available.

CloudFlare offers 86 data centers. For acceleration, this is a positive figure. It is not a direct factor in terms of DDoS mitigation, but can be important in that it does not impair the latency of your traffic or even support better regulation factors.

CloudFlare not only caters to enterprise, but also to SMB or enterprises with modest DDoS needs. It has a Business plan for only $200 monthly per site, which includes enhanced DDoS mitigation.



	CloudFlare
Diversion Method: DNS	
Always-on	✓
On-demand	✓
Non-web protocols	✗
Diversion Method: BGP	
Always-on	✓✗
On-demand	✓
Service Features	
SSL support – HSM	✗
Emergency response	✓
Fully managed service	✗
Number of data centers	79 see locations
Entry Level	
SMB plans	✓

CloudFlare has the basic DNS diversion methods.

No support in non-web protocols

Cloud has many POP. This is foremost an acceleration feature, but is indirectly important for DDoS too.

Figure 35: CloudFlare Deployment & Service Options

Mitigation

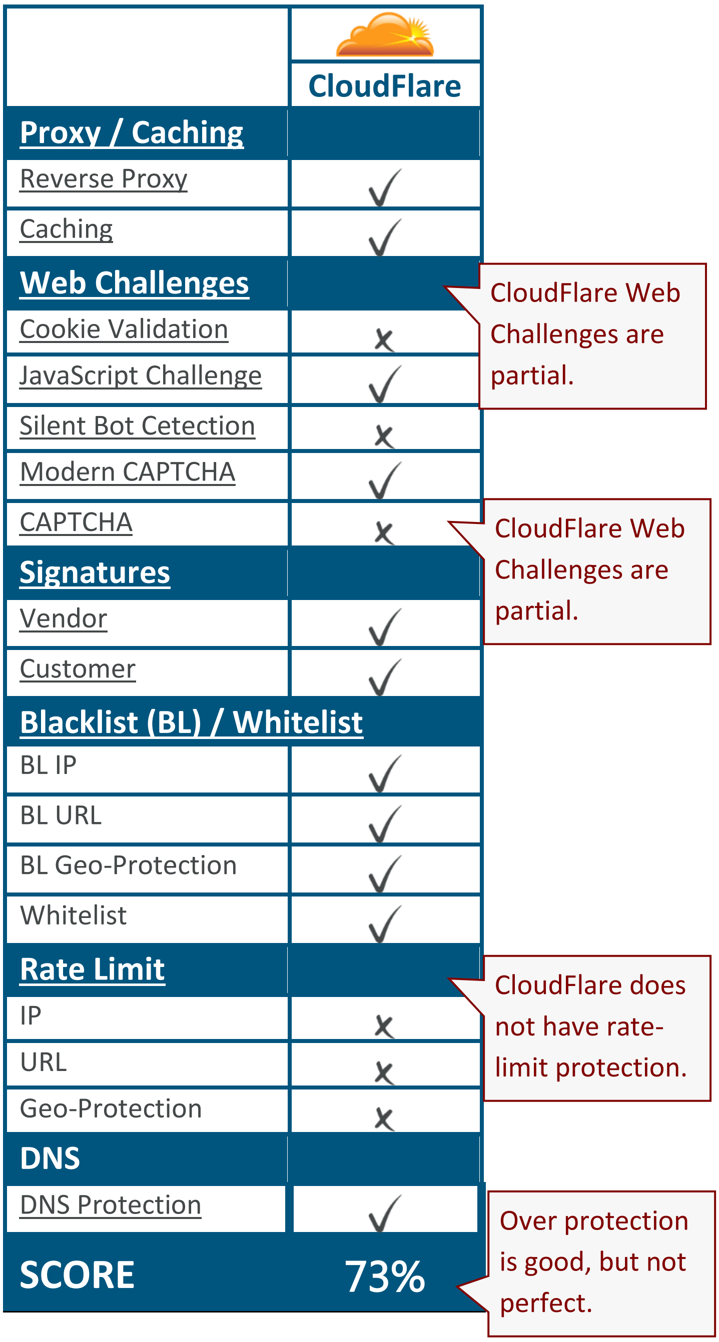
Reverse Proxy & Caching

Like with other cloud services, CloudFlare’s first line of defense is its reverse proxy and caching. This by itself blocks many attack vectors, but not all.

Web Challenges

The second, no-less-important, line of defense is the Web Challenges. CloudFlare offers a Javascript Challenge and NoCAPTCHA ReCAPTCHA, but does not have the basic Cookie Validation HTTP challenge. It also does not have the human investigation challenge (e.g., mouse movements) or the hard-core CAPTCHA (which is okay because it has the modern CAPTCHA). Therefore, it only partially provides the Web Challenge Spectrum.

Another annoying factor is that the CloudFlare JavaScript challenge is visible; the client can see that a CloudFlare challenge is occurring. It is not clear why the company does not make this challenge transparent like other vendors do. This might be some kind of advertisement for CloudFlare at the expense of its protected customer user experience.



	CloudFlare
Proxy / Caching	
Reverse Proxy	✓
Caching	✓
Web Challenges	
Cookie Validation	✗
JavaScript Challenge	✓
Silent Bot Cetection	✗
Modern CAPTCHA	✓
CAPTCHA	✗
Signatures	
Vendor	✓
Customer	✓
Blacklist (BL) / Whitelist	
BL IP	✓
BL URL	✓
BL Geo-Protection	✓
Whitelist	✓
Rate Limit	
IP	✗
URL	✗
Geo-Protection	✗
DNS	
DNS Protection	✓
SCORE	**73%**

CloudFlare Web Challenges are partial.

CloudFlare Web Challenges are partial.

CloudFlare does not have rate-limit protection.

Over protection is good, but not perfect.

Figure 36: CloudFlare Mitigation Coverage

Signatures

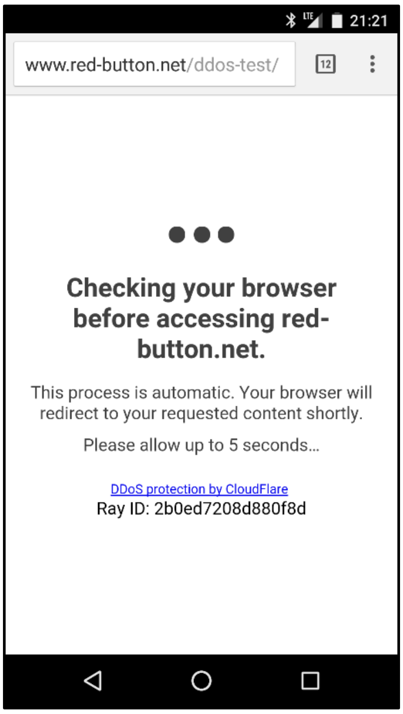
CloudFlare’s vendor signatures are very good. Unlike other vendors, the company allows you to both see and configure the signature actions, so you know what you get. Customer signatures can be created by expressing in plain English what you want the signature to be, and CloudFlare’s support will create the signature for you. However, even then you will only be able to see the signature name and control its actions, not read its exact definition. This approach may be very convenient, but with respect to our methodology it is considered a disadvantage as opposed to the user being able to directly control the signature content.

Rate Limit

Cloud does not offer rate limit at all! This has impacted the DDoS resiliency. Although it is true that rate limit is no longer a first line of defense, it is still an important one. Rate limit is important layer of defense in stopping DDoS attacks against RESTful API, where web challenges commonly cannot be used.

Infrastructure Protection

The entire Infrastructure Protection (BGP) was not available for us to review.



Checking your browser before accessing red-button.net.

This process is automatic. Your browser will redirect to your requested content shortly.

Please allow up to 5 seconds...

DDoS protection by CloudFlare

Ray ID: 2b0ed7208d880f8d

Figure 37: CloudFlare Web Challenge

CloudFlare visible and intrusive challenge. The intention here is not clear, but it acts as an advertisement for CloudFlare at the expense of its customer UX.

UX & Reporting

CloudFlare’s look and feel is good. However, it is somewhat too simple for a modern cloud service, so it is hard to fall in love with it. Still, it is definitely functional and its navigation is excellent. You can easily find your way around it.

Deployment

Deployment of a new web site (DNS) is very easy. It was not available for me to review the network protection (BGP).

All the basic security configurations are very easy to accomplish.

Real-time monitoring (RTM) was not available for me to review.

Security Events

The security events as shown on their portal are very informative and easy to review. They do not, however, send email, nor do they send a syslog. They will call you under attack and allow you to access the logs with REST API. We assume that only a limited number of users will develop a REST client just to collect the security logs.

Forensics

Forensics can start well by the detailed logs they provide in the portal. However, you will not be able to view a capture file, nor record a real-time capture file.

	CloudFlare
Look and Feel	Good
Ease of Navigation	Excellent
Deployment	
New Website (DNS)	Excellent
New Network (BGP)	Unknown
Security	
Block IP	Excellent
Block URL	Full Service
Web Challenge	Excellent
Signatures (vendor)	Excellent
Signatures (customer)	Full Service
Security	
Real Traffic	Unknown
Blocked Traffic	Unknown
Response Time	Unknown
Events	
Web Logs	Excellent
Email	✗
Call	✓
Syslog	✗
REST	✓
Forensics	
Detailed Alert	Excellent
Event Capture File	✗
RT Capture File	✗
Score	69%

CF is unique, as you can both see and control their vendor signatures.

CloudFlare does not offer email alert or syslog.

Figure 38: CloudFlare UX & Reporting Coverage

WORTH NOTING

Vendor Signatures Visibility and Control

CloudFlare is the only vendor that offers vendor visibility and control in its vendor signatures (signatures that the vendor provides to all customers). This visibility means that you can see the name of the signatures and understand what each one is protecting; you can also control its action. This is a white-box approach that this report positively acknowledges, as it provides the user with great value.

Pricing

We did not receive any pricing information or a pricing model for the CloudFlare Enterprise service level.

CloudFlare Business (for SMBs)

The CloudFlare Business plan costs $200 monthly ($2,400 annually) per web site, and gives you DDoS protection with some important limitations: no phone support, no real-time monitoring and no network protection (BGP). Despite these limitations, it provides a good DDoS entry point for organizations with clear DDoS needs but without the budget for full-fledged protection.

Next Steps – Completing your Evaluation

What have you learned by now?

DDoS Architecture

The Technical Evaluation provided you with a basic understanding on DDoS architecture options. The report is focused on DDoS Cloud Protection and you may need to read on your own about on on-premises protection, ISP based protection and Hybrid architecture. Decide on the best DDoS architecture that suites your organization's needs.

Vendor Comparison

This vendor comparison helped you compare how solutions differ in their Deployment & Service Options, Mitigation, UX and Reporting, and understand Which Solution is Right for You?, based on your needs.

Additional vendors

The report currently covers only three vendors. Using your knowledge you should now be able to investigate additional solutions till we add more vendors in the future.

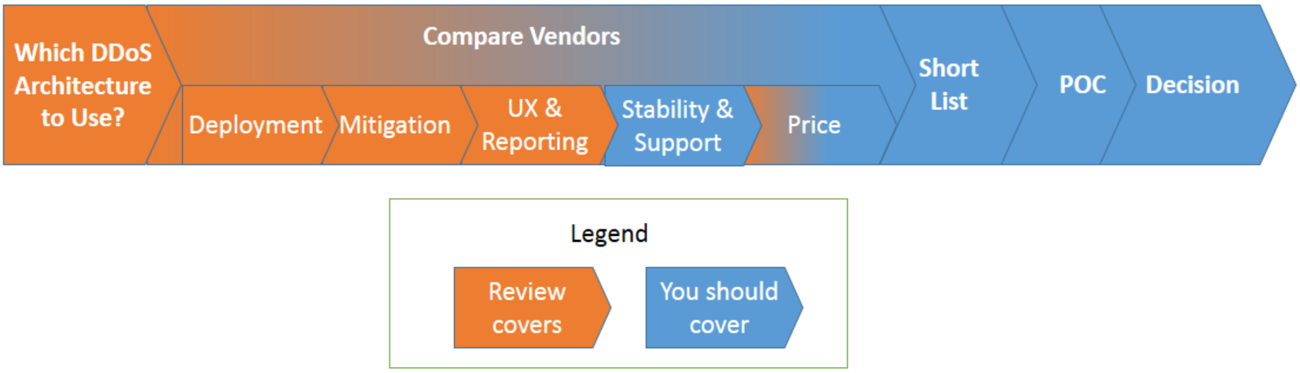


Figure 39: DDoS evaluation process and remaining tasks

What's next?

Stability and Support

Stability and support are critical factors, but were not cover in our report. Next you should try and evaluate these aspects on your own.

Mission Critical Services May Suffer Stability Issues in Cloud Services

It is common knowledge that all cloud-based services may have stability issues that are the result of a multi-tenant environment. The main problem is that an enormous attack on one tenant can affect another tenant. Stability should be a key factor for organizations with mission critical services, that rigorously monitoring their service and cannot tolerate short outages or latency. it is recommended to validate stability with potential vendors, determine their reputations and conduct longer POCs.

Pricing

Most vendors keep pricing very private.When you get quotes from vendors, make sure that they are provided in a manner that will allow you to compare apples-to-apples.

POC

Old-timers know the POC (Proofs of Concept) can lie more than tell the truth. The main goal in POC is to take you from the theoretical data sheets to the practical, hands-on experience, and enable you to make a more educated decision.

Another approach is to purchase the service for a limited time or in buy-or-return model and integrate it in your production. This approach is not always possible, but it is more productive than a POC.

Decision

At this point you should have enough input to make a decision.

Glossary

Always-on

See Always-on versus On-demand

Always-on and On-demand

'Always-on' and 'On-demand' are two opposite terms referring to the DDoS mitigation cloud service. In an Always-on deployment, the service or network is constantly being protected by the DDoS mitigation service, while in On-demand there is no protection most of the time, and the DDoS mitigation layer is inserted only under a DDoS attack or severe threat.

For example, when using DNS diversion, clients reach the protected service directly and only under an attack. The DNS records are being changed to direct all traffic to the DDoS service provider.

Always-on protection is much faster and more reliable under attack. The advantage of On-demand deployment is that the DDoS layer is used only when needed and is commonly cheaper.

BGP Diversion

BGP Diversion is a DDoS cloud protection technique in which an organization is able to divert its traffic to the DDoS provider using a BGP announcement. This method is applicable only to organizations that possess a C Class network and that can advertise it via BGP. To divert the traffic, both customer and provider change the BGP announcement to indicate to the entire Internet that the custom IPs should be routed to the provider data centers. BGP diversion can be Always-on or On-demand. It is more complicated DNS diversion, but it has security advantages, since it can provide infrastructure protection.

Related entries: DNS Diversion, Infrastructure Protection, Web Protection

Blacklist / Whitelist

Blacklist and whitelist are two technologies that are often used in tandem. Blacklist is the ability to block an entity such as a user-based IP or an entire network range or geographical location. Whitelist is the opposite – it allows a certain entity to pass even if the other technologies have decided to take action against it. Both technologies maintain an important role in DDoS mitigation.

CAPTCHA

CAPTCHA or CAPTCHA Challenge is a type of Web Challenge. CAPTCHA stands for 'Completely Automated Public Turing test to tell Computers and Humans Apart'. It is challenge intended to differentiate between computers and humans.

Computers generally are unable to solve the CAPTCHA and state the word and letters, while humans are.

CAPTCHA is used to mitigate DDoS attacks, as legitimate users are able to pass it, while attacking computers cannot. Nevertheless, CAPTCHA is not the most popular DDoS web challenge because it is very intrusive and has a negative effect.

Related entries: Cookie Validation, Modern CAPTCHA, Web Challenges, Web Challenge Spectrum

Cloud Protection

See Cloud protection vs Appliacne Protection

Cloud Protection and On-Premises Protection

DDoS mitigation can arrive in two main forms: Cloud-based and On-premises. On-premises protection is when the DDoS mitigation technology is located inside the customer premises, typically as an appliance or a virtual appliance. A protection outside the customer premises is called Cloud Protection. Oganziations use cloud-based protection by diverting their traffic to the cloud data centers where the DDoS mitigation technology resides and cleans the DDoS attack before sending clean traffic back to the organization. ISPs providing DDoS Protection are also considered as cloud protection in the broader sense as they are able to protect an organization's internet pipe.

Related entries: Hybrid Protection

Cookie Validation

Cookie Validation is a type of Web Challenge that is used in DDoS mitigation to filter out attackers from legitimate clients. The challenge is to send every client, attacker and legitimate user a web cookie and to request that the client send it back (typically using the HTTP 302 Redirect command). A virtually legitimate browser supports web cookies and will easily pass the challenge transparently (without the user involvement), while DDoS bots typically don't save cookies and therefore cannot pass the challenge.

Related entries: JavaScript Challenge, Web Challenges, Web Challenge Spectrum

Customer Signatures

See under Signatures.

Customer-Oriented Pricing Model

Pricing models of DDoS cloud mitigation are quite similar, but it is important to understand the differences between them. From a customer point of view, a pricing model should be simple and easy to understand. It should also be flexible so that you don't pay for services that are not required.

With these assumptions, the factors that should be used in the DDoS pricing model are traffic volume, the number of protected web servers, and the number of data centers. It is easy to understand why all of these factors reflect the genuine size of the service, its cost to the provider and its price to the customer. Using the same logic, other factors that should affect pricing are a fully managed service versus semi-managed or self-service, and always-on versus on-demand service.

It seems that the five factors covered so far should be enough, but another pricing factor used by vendors is 'attack traffic rates.' This is a parameter that confuses customers, and is likely to lead to either over-pricing or under-protection. Most customers are not familiar with attack rates. Even if they are, no one can predict the future and plan for, say, a maximal of 10G attack. Providers, of course, should have the right to charge more for a customer that is attacked more often, like those in the gaming industry. Some providers are setting maximal hours of mitigation under a fair usage agreement. Ninety-five percent of customers will never cross this fair usage and should never worry about it.

DDoS Appliance

A DDoS appliance, also referred to as a dedicated DDoS appliance, maintains as its primary function DDoS mitigation. A DDoS appliance can be either virtual or physical. IPS and WAF often also have DDoS mitigation capabilities; however, it is not their main function and generally they are not as complete as DDoS appliances.

Related entries: WAF Appliance with DDoS

DNS Diversion

DNS Diversion is a type of DDoS cloud protection technique in which an organization is able to divert its traffic to the DDoS provider using a DNS change. The change is as simple as modifying the relevant DNS record so that they will eventually direct traffic to the provider's IPs. DNS Diversion can be always-on or on-demand. The provider is then able to mitigate the DDoS attacks and send the clean traffic back to the customer.

DNS Diversion is simpler than BGP Diversion but has limitations, such as protecting the origin IP.

Related entries: BGP Diversion, DNS Diversion, Infrastructure Protection

DDoS Forensics

DDoS Forensics is the digital forensic process to better understand a DDoS attack. Forensics can be done for past attacks but also for ongoing attacks. The output of forensics can shed light on the attack vectors, attack tools and the attacker characteristics or identity. The goal of DDoS forensics is to gain visibility that will help you mitigate an ongoing or future attack. For example, if you realize that attackers are using the LOIC tool against you, you can expect additional attack vectors used by this tool. In addition, forensics are used in an attempt to locate attackers, which in DDoS is not an easy task.

DNS Protection

DNS Protection refers to the ability of a DDoS mitigation provider to mitigate DDoS attacks. This can be done using DDoS mitigation technologies or by moving the organization's DNS records to the provider DNS server that is strong enough for DNS floods.

Emergency Response

A team of experts that can help customers while under DDoS attack to identify, analyze and mitigate the attack. Under attack this team will validate that your site is fully protected. If not, it will enable additional protection or fine-tune existing protection until the attack is mitigated.

Entry Level

A DDoS entry-level plan is intended for SMBs or enterprises with modest DDoS needs. We have defined the bar at $5,000 USD annually. Entry level will typically give you protection based on DNS diversion, which is sufficient to protect your web site. Entry level typically does not include BGP diversion, real-time traffic reporting or phone support, and for this reason most enterprises cannot use this service plan.

Forensics

See DDoS Forensics

Full Service

A product or service function is referred to as Full Service if the customer cannot use or change this function independently and must request it from the service provider. Full service is in contrast to Self-Service, and generally is a negative trait, since it is betterto give direct control to customers via self-service.

Related entries: Self-Service

Fully Managed Service

Fully managed service is a service in which the customer is not required to perform any action to be fully protected and the vendor is responsible for the initiation of the security process. Let's take as an example a security event that occurred during the weekend. In a fully managed service, the responsibility to investigate it, produce a report, plan action items and execute them falls on the service provider and not the customer.

This definition can be tricky, as many DDoS providers that are not fully managed are provided with a partially managed service, such as taking on the responsibility of mitigating an ongoing attack. Other providers who declare themselves fully managed may still shift responsibility to the customer.

HSM

A hardware security module (HSM) is a physical computing device that safeguards and manages digital keys for strong authentication and provides cryptoprocessing. In DDoS mitigation cloud services, HSM is used to securely upload a sensitive certificate to the provider. The provider requires your certificate so it can scrutinize it for DDoS attacks inside the encrypted traffic. Some providers do not have HSM as part of their service, and therefore there is some risk in providing them with a most sensitive asset such as the certificate. The HSM reduces this risk.

Hybrid Protection

Hybrid protection is a DDoS protection approach that includes both cloud protection and on-premises protection - most commonly, but not necessarily, delivered by the same vendor. The advantage of this DDoS architecture is that it enables you to mitigate each attack vector in its optimal location.

Related entries: Cloud protection vs on-premises protection.

Infrastructure Protection

See Web Protection and Infrastructure Protection

IP Protection

IP Protection is a method that enables protecting non-web services without using BGP. It addresses the problem of organizations that do not own a Class C network and are therefore unable to use BGP diversion Using IP protection, a service provider provisions the customer an IP out of its own Class C network. Instead of using the customer's Class C, the provider’s Class C is used. From here, the diversion continues like any other BGP diversion, and will commonly have a GRE tunnel to route traffic back to the customer.

IP Protection—and this is an important point to clarify—does not directly solve the attack problem because an attacker can still learn the organization's IPs and attack them directly. However, just like in DNS diversion, there are workarounds to reasonably close this attack vector.

An alternative method that addresses the inability to use BGP diversion is L4 proxy.. However, the number of vendors that offer an L4 proxy solution to the problem is still limited.

JavaScript Challenge

JavaScript Challenge is a type of Web Challenge that is used in DDoS mitigation to filter out attackers from legitimate clients. The challenge is to send every client, attacker and legitimate user a JavaScript code that includes some kind of challenge. Virtually any legitimate browser has a JavaScript stack and will easily understand and pass the challenge transparently (without the user’s notice), while DDoS bots typically are not equipped with JavaScript stack and therefore cannot pass the challenge.

Related entries: Cookie Validation, Web Challenges, Web Challenge Spectrum

Look and Feel

Look and feel is the overall impression a service maintains and is based on both the organization of content and graphical design. A good look and feel increases usability and productivity.

Number of Data Centers

The number of data centers, also referred as POPs (points of presence) or ‘scrubbing centers’, that a vendor offers has no direct impact on the DDoS mitigation but may still be very relevant in the following cases:

Improve latency – some organizations have CDN requirements from the DDoS cloud service,which may be more importantthan the DDoS mitigation features.

No impact on existing latency – An organization that wants to ensure the cloud diversion does not impact the existing latency will validate during deployment the number and location of data centers.

This is relevant for organizations that are planning to use the service in an always-on mode. Organizations using an on-demand service are less sensitive to the number/location of data centers, unless they are constantly under attack.

Non-Web Protocols Support

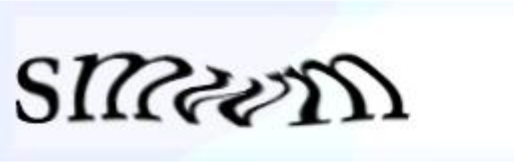
Non-web protocols support refers to the ability to protect non-web protocols (e.g., proprietary gaming protocols) even if the organization does not poses a Class C network. An organization that posesses a Class C network can divert the traffic to the provider using BGP. Otherwise, in most cases it is not possible because many vendors allow only an L7 web-based proxy. An L4 proxy is not supported. This leaves proprietary protocols unsupported and at great risk.

Modern CAPTCHA

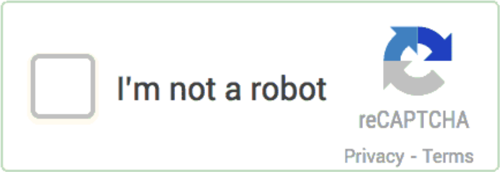
Modern CAPTCHA is a type of challenge intended to differentiate between computers and humans.

Modern CAPTCHA address the shortcoming of the traditional CAPTCHA,namely thathumans are also having trouble to pass them successfully. NOCAPTCHA ReCAPTCHA is the most prominent example of modern CAPTCHA.

Related entreis: CAPTCHA, Web Challenges, Web Challenge Spectrum



CAPTCHA



Modern CAPTCHA
(NOCAPTCHA ReCAPTCHA)

On-Demand

See Always-on and On-demand

On-Premises

See Cloud protection and On-premises protection

Peace Time

In DDoS, 'Peace Time' refers to the period during which your organization is not under attack and your DDoS mitigation service is expected to be quiet, stable, and causing no false alarms.. Peace Time is in contrast to 'War Time'.

Related entries: War Time

Rate Limit

Rate limit is a technology used in DDoS mitigation, which ensures that each individual asset does not make too many transactions to the protected server or network. For example, each IP cannot make more than five HTTP requests per second. Rate limit is effective in keeping the service safe from many variations of DDoS. However, it is not considered a first line of defense because it can cause false positives. In certain situations such as a web API rest, it may even be the first line of defense.

Reverse Proxy

See Web Reverse Proxy.

Reverse Proxy and Caching (DDoS Mitigation Technology)

Reverse Proxy (Web Reverse Proxy) and Caching are two different technologies that often come in tandem, especially in DDoS.

The reverse proxy acts as an effective DDoS layer, as it is located between the attacker and the targeted server. Virtually all the network attacks directed at the server will hit a wall when they reach the reverse proxy.

Caching resides on top of a reverse proxy and stores web pages on the proxy. During a DDoS attack, numerous requests to a single resource will result in only a single request to the server, so that it will not experience the impact of the attack.

When the two technologies are combined, they block virtually all the network attacks, application attacks to static pages and to some degree, other types of attacks. This technology combination is considered one of the most effective methods against DDoS.

Related entries: Web Reverse Proxy

Signatures

Signatures—also called 'DDoS Signatures' or 'IPS DDoS Signatures'—refer to a significant DDoS mitigation technology in which DDoS attacks are detected and blocked based on their known patterns. For example, the famous Anonymous tool LOIC (Low Orbit Ion Canon) carries a certain pattern that a signature can block.

Signatures are divided into two types: vendor and user. Vendor signatures come in large numbers and are based on vendor research. User signatures are created by the user, typically during or after an attack. Both maintain an important role in DDoS mitigation.

Self-Service

A product or service function is referred to as Self-Service if the customer can use or change it independently without having to request it from the service provider. Self-Service is in contrast to Full Service, and generally is a positive feature, since it provides direct control to the customer.

Related entries: Full Service.

Silent Bot Detection

Silent bot detection is an advanced web challenge technology to detect bots by sending JavaScript code that does passive and proactive checks to validate if the client is a human or a bot. This can include checking for the existence of mouse and keyboard, checking if the browsers features resembles a browser used by real users and more.

Related entries: Web Challenges, Web Challenge Spectrum

SMB Plans

SMB plans refer to plans covered in this report that include DDoS protection and are priced lower than $5,000 annually. Such plans are much cheaper than enterprise plans but include only a subset of the functionality. They'll typically include DDoS mitigation, Web Protection and security logs, but no Infrastructure Protection or phone support and therefore, the emergency response will be partial.

Subset of Services Business Plans Receive	
Web Protection	✓
Infrastructure protection	✗
DDoS mitigation	✓
Security logs	✓
Real-time reporting	✗
Phone support	✗
Emergency response	✓✗

SMB plans include only a subset of the enterprise plans.

Vendor Signatures

See Signatures.

WAF Appliance with DDoS

The Web Appliaction Firewall (WAF) appliance is a security appliance that protects web servers from many types of attacks, and include DDoS mitigation features. A WAF can be either physical or virtual.

Related entries: DDoS Appliance

War Time

In DDoS, 'War Time' refers to the period during which an organization is under attack and the DDoS mitigation service is expected to mitigate the attack. War Time is in contrast to 'Peace Time'.

Related Entries: Peace Time

Web Caching

A web cache (or HTTP cache) is technology for temporary storage (hence, caching) of web content. The technology is used to reduce the load from web servers, reduce bandwidth usage and improve acceleration.

When used in tandem with web reverse proxy, caching is an effective layer against DDoS because many attack vectors will by captured by the web proxy and caching server and will fail to reach the web server. This is true for static requests, while some dynamic requests and other attack techniques are capble of bypassing this line of defense.

Related entries: Reverse Proxy & Caching DDoS Mitigation Technology

Web Challenges

Web Challenges include several technologies used to distinguish between real humans and bots, or DDoS bots in our context. The best-known challenge is CAPTCHA, which is very intrusive.Other, less-intrusive transparent challenges include Cookie Validation or the JavaScript Challenge. Web Challenges are considered one of the most effective mitigation layers against DDoS application attacks.

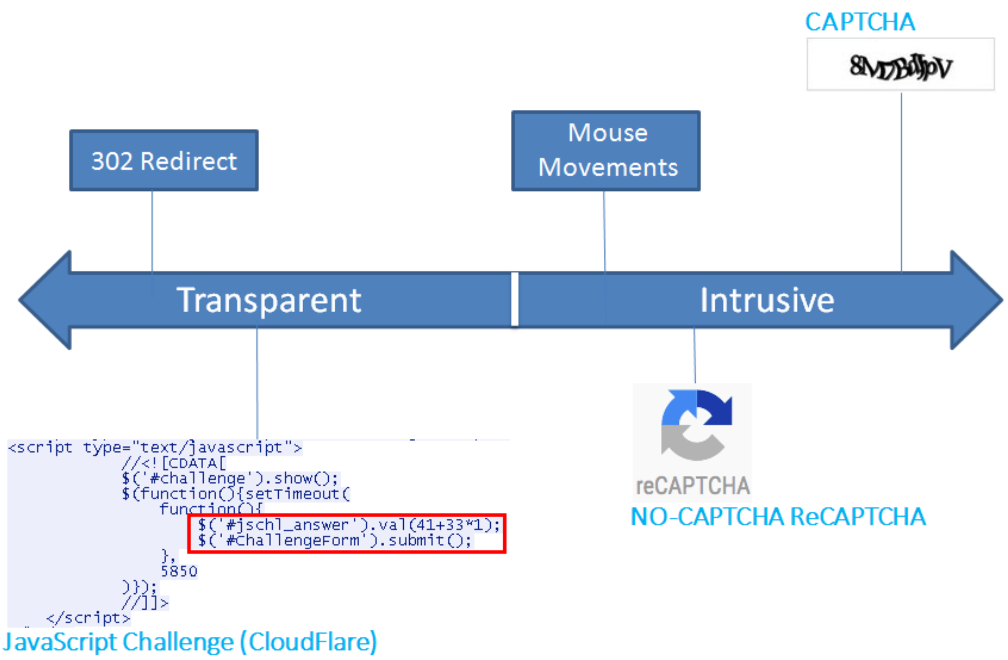
Related entries: Cookie Validation, JavaScript Challenge, Web Challenge Spectrum

Web Challenge Spectrum

Web challenges are one of the most effective ways to stop web-based DDoS attacks. Some challenges are transparent to users, yet block significant types of attackers. Others are very strong and do not allow any bot to pass, yet do so at the cost of being more intrusive to legitimate users. Ideally, vendors should offer as many types of challenges as possible to allow customers to use the most suitable challenge to their situation and goals.

Perhaps the best-known challenge is the **CAPTCHA**. CAPTCHA’s intention is to allow only humans to pass, while blocking bots. Therefore, it can stop DDoS attacks originating from bots. In reality, CAPTCHA is hardly used against DDoS attacks, although it is extremely effective against bots. The reasons is that it is unfriendly to humans and often users have trouble passing the CAPTCHA causing some users leave the website. The more popular challenges for DDoS mitigation are the “silent” challenges. For example, **Cookie Validation** sends users a redirect command with a special cookie, expecting the client to return the cookie. This simple challenge is easily passed by a browsers will actually fail most bots.

Related entries: Cookie Validation, JavaScript Challenge ,Web Challenges,



```
<script type="text/javascript">
            //<![CDATA[
            $('#challenge').show();
            $(function(){setTimeout(
                function(){
                    $('#jschl_answer').val(41+33*1);
                    $('#ChallengeForm').submit();
                },
                5850
            )});
            //]]>
    </script>
```

Figure 40: Challenge Spectrum

The ‘**JavaScript Challenge’** is the ‘older brother’ of Cookie Validation. While in the Cookie Validation the challenge was implemented in HTTP, now it is implemented in the JavaScript (JS) language. To pass the challenge, attackers would need to ‘speak’ JS, which few bots today do.

Some challenges conduct additional investigations to determine humans and bots. They issue checks for mouse movements and the existence of a keyboard as well as other signs indicating whether the user is a human or a bot. These type of challenges are referred to as ‘**Silent Human Investigation**’.

If all the silent web challenges are not effective, one can always escalate to the CAPTCHA sledgehammer or the lighter hammer version of **NoCAPTCHA reCAPTCHA**.

The different types of challenges are referred as the Challenge Spectrum because in different situations you may want to use different challenges. In some situations you may settle on a light-weight, transparent Cookie Validation, while in others you may need to stop an attack with a CAPTCHA.

Related entries: Web Challenges

Web Protection and Infrastructure Protection

Cloud-based DDoS mitigation services offers two primary protection types: web protection and infrastructure protection. Web protection is the ability to protect web sites and web based services typically by means of DNS diversion. Infrastructure Protection is the ability to protect the direct attack on the organization IP or Network, typically by means of BGP diversion.

Related entries: BGP Diversion, DNS Diversion

Web Reverse Proxy

'Web reverse proxy' or, in short, 'reverse proxy', is a server that receives the client's request and then passes the requests to the web server. When the proxy is strong enough, it acts as an effective DDoS layer, as it reduces the attack surface andmitigates virtually all the network attacks that cannot reach the protected server.

Reverse proxy commonly comes in tandem with caching, which reduces even further the attack surface and in particular, also blocks application attacks.

Related entries: Reverse Proxy and Caching DDoS Mitigation Technology

Appendix

Research Methodology

Overview

The goal of this report is single: to help organizations choose the most appropriate vendor for their environment. To do so, the following guidelines were used:

- **Technical focus**
  The analysis is focused on a technical analysis rather than a business one.
- **DDoS features only**
  All vendor reviews here provide much more than DDoS: CDN, WAF, load-balancing and more. This repot focuses only on DDoS.
- **War-time evaluation**
  There is a great emphasis on the services' performance under attack, in their money-time, in addition to daily peace usage.
- **Cooperate with vendors**
  Reviewed vendors were approached. They were asked for information and evolution licenses, and were also asked to comment on the report prior to its publication.
- **Source of information is public documents, hands-on and vendors**
  The report is based on public documents, hands-on experience with the products and feedback received and verified by vendors. DDoS or any lab testing was not included.
- **Break-down method: (1) Deployment, (2) Mitigation, (3) UX & Reporting, (4) Stability & Support and (5) Pricing**
  This break-down method was used to analyze each vendor. A scoring system was developed for each section to score each vendor.

Cooperation With Vendors

In this report, interaction with the vendor plays a great role. Each vendor was asked to provide a focal point to collect technical and business materials and to answer inquiries. In addition, an evaluation, or at least a demo, was requested.

	Incapsula	CloudFlare	F5
Proxy / Caching			
Public materials	✓	✓	✓
Vendor cooperation	✓		✓
Demo	✓		✓
Hands-on	✓		

Figure 41: Level of Cooperation With Each Vendor

Incapsula and F5 cooperated with our research, while CloudFlare did not. This is the reason for some missing aspects regarding CloudFlare's analysis.

Technical Focus

The analysis is focused on a technical analysis rather than a business one.

This is not the first DDoS report out there. The Forrest's DDoS Services Providers, Q3 2015 (or obtain it free of charge here) is methodological and worth reading. However, it takes a ten-thousand-foot view and presents more business-oriented aspects, like market size and global presence. While these factors are important in the vendor selection process, our approach is a more technical. In particular, we examine deployment factors and mitigation factors. Another competitive analysis is Top-10 DDoS Protection Services Reviews. This analysis provides a good introduction for beginners; however, the analysis itself is very flat and includes no DDoS features.

DDoS Features Only

Only DDoS features are reviewed; CDN and generic WAF are excluded.

The report reviews only DDoS mitigation capabilities. Although some of the vendors offer an internet acceleration Content Delivery Network (CDN), Web Application Firewall (WAF) or other interesting technologies, they are all disregarded unless they have any DDoS mitigation value. In reality, organizations may add no DDoS-related aspects to their overall decision.

War-Time Evaluation Focus

Products will be evaluated here with a greater focus on how they perform under attack than in peace time.

Perhaps the biggest problem with DDoS is that peace time can last as long as one to two years, creating the sensation that everything works well. This report is mostly concerned with how thing will work in war time. Will the attacks be blocked? What kind of visibility and control you will get? Will there be false positives?

Source of Information

Data is based on vendors' public materials, discussion with vendors and a user interface review.

The report does not include testing and/or the reputation of the vendor. As mentioned above, for vendors that have fully interacted with the research, a detailed analysis is presented as is a competitive analysis. For the rest, only a basic analysis is provided

ADDITIONAL ITEMS

Weight-Based Evaluation

The report a priori assigns weights to different features based on their estimated value to customers.

There are literally hundreds of features that can be reviewed in DDoS mitigation. We have a priori selected the features we consider most important and have assigne a weitght to each. Our weight system is based on the weights we think customers should assign to each feature.

The weight-based system gives our analysis two advantages. The weight system forces the evalution to focus on the important features on which we decided a priori. For example, the branding of the vendor has no importance because branding was decided a priori to not be a factor.

The weight system also boosts the objectivity of the report. With it, the review becomes a technical job of marking each vendor according to which features exist (and to what extent) and which do not.

Note that some aspects of the service that we considered important are missing simply because we were not able to objectively measure them. This includes the stability of the service and the support level. In many cases, we did not have access to pricing. The aspects we were not able to cover are stated passed for the organization to complete, as indicated in the Next Steps – Completing your Evaluation section; we still plan to cover them in the future.

Existing Features Only

The analysis ignores the vendor's roadmap; only existing features are evaluated.

The organization's roadmap is not included in the analysis. This report evaluates only what is out there at the time of analysis. It is planned to update the report on a regular basis.

Break-Down Method

There are so many aspects of DDoS solutions. To create order in this domain, the analysis is divided into five parts.

We were able to cover the first three rather well. Stability & Support has not been covered well so far. (We are planning to complete this in the future.) Pricing was covered partially because not all vendors provided it.

What makes a good DDoS service?
Setup & Deployment
Mitigation
UX & Reporting
Stability & Support
Price
DDoS

Decent Disclosure

The **DDoS Vendor Review** goal is to help organizations choose the best DDoS solution for them. It includes reviews of DDoS vendors, with a strong focus on their technical merits.

The following describes how the analysis is done, how it is funded and what measures are used to keep it objective.

Objectivity

The analysis's ultimate goal is to help organizations choose the best DDoS product. Red Button's assumption is that product selection is one of the biggest issues organizations face today in DDoS mitigation, perhaps the biggest one. Organizations face an information gap in making this critical decision.

To meet this goal, the report must be objective. This is achieved by a funding method that does not affect the content.

Funding

The primary funder of the report is Red Button itself. Red Button offers multiple DDoS services, including consulting, training, DDoS simulation, managed services and more. Red Button is not a DDoS vendor and therefore the analysis scope excludes its own activities.

The secondary resource for funding the report is selling SEO and marketing benefits such as retargeting pixels or links to vendors' web sites. This activity does not, implicitly or explicitly, affect the content of the analysis.

Interaction with vendors

Red Button interacts with multiple vendors on a daily basis. In some cases there may be business-related interaction (e.g., Red Button can act as a reseller of a vendor for a given customer). However, Red Button maintains a strict vendor-neutral approach, and intimate interaction with the vendor is considered an asset, as it is used to validate the vendor's claims.

Cooperation with vendors in the analysis

Red Button strives to cooperate with all selected vendors. The vendor's cooperation includes the following: request for public information, evaluation license and request for comments on the analysis draft.

Some of the vendors cooperated very well, while others did not. In the latter case, this impairs our ability to present a complete analysis and to include the vendor in the competitive analysis section.

About the Author

Ziv Gadot

Ziv Gadot is Red Button's founder and CEO. Red Button is a consulting and services company that prepares organizations for DDoS attacks from an architectural vendor-neutral point of view, and ensures that the organization conducts all the necessary steps to be prepared: gap analysis, DDoS simulation test, technology selection, SOC training and emergency response.

Prior to Red Button, Gadot worked at Radware for 11 years. He had founded and managed Radware's Emergency Response Team (ERT), a 24x7 response team that helps organizations that under DDoS attack. Prior to that, he worked on Check Point's VPN team and at Intel. Ziv has a BA in CS from Technion, Israel Institute of Technology, and an MA in Philosophy from Tel Aviv University. He is a frequent speaker at security conferences and the author of security reports.

Feedback

Feedback on this report is welcome and should be sent to ddos-analysis@red-button.net

RED BUTTON
DDoS EXPERTS

About Red Button

Red Button is a security services and consulting company specializing in Distributed Denial of Service (DDoS). We have helped mitigate hundreds of DDoS attacks on banks, stock exchanges and governments, and use our expertise to provide preemptive and emergency response services to organizations of all sizes. Our services include DDoS readiness evaluation, penetration tests, technology selection, consulting, SOC training and emergency response. Red Button has also established the DDoS Resiliency Score (DRS) standard, which helps companies evaluate their DDoS attack readiness in objective, quantitative terms. For more info about Red Button, see www.red-button.net.

www.red-button.net