WHITEPAPER

INDUSFACE™

Managed **Cloud WAF** is a must have for Growth

No matter how much you look for alternatives, managed WAF is the best solution available to protect applications from attacks. With AppTrana you will finally get a Cloud WAF.

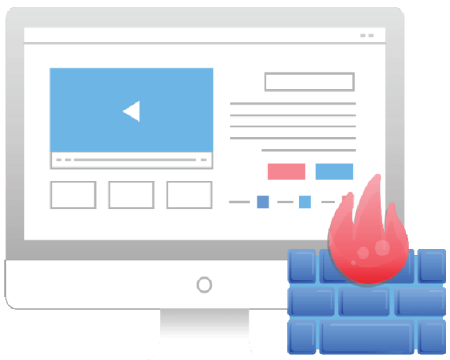
MANAGED CLOUD WAF IS A MUST HAVE FOR GROWTH

Web Application Firewall (WAF) has been around for decades. According to Wikipedia, early commercial versions of WAF were seen as early as the late 90s. In the early 2000s, ModSecurity was formed to improve the accessibility of WAF, it created rules based on the OWASP TOP 10 vulnerabilities, which became the basis of security compliance in years to come.

In 2006, PCI DSS 1.1 was released which added an important clause – Requirement 6.6 which stated, "all custom application code must be professionally reviewed for vulnerabilities or a web application firewall must be installed in front of web-facing applications,"[1]. This requirement saw a rapid explosion of WAF as it not only was just a good security tool but also an enabler of compliance. WAF became mainstream and primary tool for application protection. Growth of the WAF market was exponential with various vendors providing various flavors of WAF. According to Gartner, the WAF market alone was around ~1 billion dollars at the end of 2019.

With more than two decades of growth, one would imagine that the WAF market should have been matured by now with WAF becomes an effective tool for protecting applications over the internet. This also means hackers should by now be having a hard time bypassing WAF and breaches should be declining and becoming a thing of the past. Unfortunately, reality cannot be farther away than this. One of the recent surveys from Neustar International Security Council[2] stated that 4 in 10 respondents say 50% of attacks bypassed WAF. 3 in 10 say 50% of requests were marked as false positives. This is also backed by another research by Ponemon Sullivan[3] where stats are most astounding, nearly 60% of the organizations are dissatisfied with WAF and only 22% of organizations have WAF in block mode.

Why is the case? what is ailing the WAF market? Is ML the holy grail for application security that it was is touted for? and how can WAF be effectively deployed to ensure better efficacy? This is what we will try to explore here.



WAF and Its Challenge:

WAF is a secure gateway for applications, especially for those accessible over the internet. When WAF is deployed before an application, all traffic to the application is routed through the WAF gateway that inspects the traffic for any malicious requests and blocks them. This sounds simple and seems to be an extension of a network firewall that inspects network traffic. Well, true, but probably the similarities stop there.

The concept of identifying malicious requests is where the challenge arises. There is no silver bullet to identify if a request is malicious. Generally, WAFs work on either a positive security model or a negative security model.

- **Positive Security Model -** In case of a positive security model, as the name suggests traffic is observed and only that meets certain criteria is allowed, all other requests are blocked.
- **Negative Security Model -** The negative security model is the reverse of the positive security model, where traffic is observed and if a certain characteristic is observed then the request is blocked else traffic is allowed.

Most WAF vendors take a hybrid approach. Initially mostly negative security model was what used, where rules were written based on malicious patterns, then positive security model was touted to be the way to go, (i.e.) learning the characteristic of sites and blocking all requests that don't meet the normal behavior.

No matter what the approach was taken the challenge was/is around coming up with a model to accurately identify the characteristic of the request and compare it with the characteristic of the site to determine the legitimacy of the request. This model needs to finely balance between false positives (FP - blocking legitimate requests) and false negative (FN - allowing illegitimate requests).

Due to this inherent nature of WAF, it leads to a constant tussle between availability and security. Web application owners need security, but not at the cost of business if any legitimate traffic was blocked it leads to a loss in business and this was not acceptable. It is because of these reasons that WAF efficacy always comes into question. If you talk to anyone who understands the WAF market, they will talk about these challenges:

- **Lack of Proper Protection:** Nearly 65% of WAF deployments can be bypassed, this is mainly because of the tussle between FP and FN's. In order to reduce FPs, WAF rules are tuned to be less effective which means actual attacks are not blocked. One of the primary reasons for this is because of lack of security expertise to fine-tune the rules effectively.
- **False Positive:** Applications are constantly changing, this means rules need to be monitored constantly, organizations do not have the expertise or bandwidth to do the same which leads to FPs.
- **Intent:** As I discussed earlier, the major driver for WAF deployment is compliance, but because that is the only intent, in most deployments, the efficacy of WAF is only on paper. In most organizations WAF deployment is only in log mode, providing alerts for offline intervention, but most times the alerts are huge with a lot of FPs making the alerts ineffective as it is not easy to filter out actionable alerts from the noise.
- **Resource-hungry deployments:** WAF deployments are complex, resource-hungry, and costly. On-Premises deployments come with huge upfront CAPEX and are very complex to maintain. In fact, according to Ponemon, WAF management requires an average headcount of 2.5 and an annual budget of over $400K.

Is Machine Learning the Holy Grail?

As the market is around for more than 2 decades, there have been many solutions over various period that was/is projected as a silver bullet to these problems. The current fad is machine learning.

Are machine learning and artificial intelligence the holy grail? The answer is yet to be determined. But what one needs to understand is, as of today there is no holy grail available. Most machine learning that is out there in the market is at best in learning mode all the time or at a worst ineffective causing lot of FPs.

Machine learning is not becoming mainstream in the application security space because of the ever-changing nature of applications, security, and threat landscape. Unsupervised learning needs a huge set of data for the model to become accurate, but unfortunately as applications keep changing, by the time it learns and understand a pattern the application changes, traffic pattern changes, attacks evolve. As new technology comes into the picture, the same technology is also available to hackers, so they are also evolving and can create attacks that can trick the learning algorithms to create back doors.

It is not to say, machine learning won't catch up and evolve to be a more effective solution than it is today, but we are still far away.

Is WAF the only option?

No matter how many new solutions are projected as the next best thing to protect the application without any human intervention, WAF is by far the most effective and scalable solution that is available.

RASP which is projected as an alternative is not scalable. The effectiveness of RASP is majorly dependent on the hooks it has to the application which makes it implicit and tightly coupled with the language in which the application is written. RASP that claims itself to be language agnostic is pretty much a poor man's WAF deployed as a wrapper on the server instead of a separate proxy in line with the application server. RASP because of its nature of deployment is not an effective protection against attacks like DDOS attacks.

So, no matter how much you look for alternatives, WAF is the best solution available to protect applications from attacks.

How Do You Secure Your Application with WAF and Reduce Risk?

Though WAF comes with its challenges, if you look deeper, WAF's effectiveness is directly dependent on how well it is configured. So, it more or less comes down to selecting the right WAF vendor and the process you have in place to ensure WAF is effective. To effectively deploy WAF you need to do the following things right:

- **First, choose the right deployment model.** With everyone moving to the cloud you need a vendor who understands the cloud ecosystem well and grown bottom-up on the cloud. Cloud WAF is highly scalable and does not need you to spend upfront Capex on infrastructure. Shackles around data privacy no more hold, right vendors know how to store the data securely adhering to the data privacy rules of the nation you reside in. Cloud WAF is also very effective around DDOS protections and ensures you don't need to spend time maintaining the infrastructure.

- **The next part would be choosing the right vendor.** You don't need someone to provide just out of the box and provide complex controls that are expected to be configured by you. Application security is complex, to configure WAF you need to walk on a tight rope by balancing FPs and FNs. If the vendor just provides you set of default rules and expects you to fine-tune them based on application need, you are in for a challenge. Applications keep changing, every deployment needs monitoring of the rules, and if any rules misbehave, they need to be tuned. Any update by the vendor on the default rules can affect the application functionality. So, you will need to be constantly in vigil, monitoring application functionality, WAF triggers ensuring WAFs are not misbehaving. This may work if you have a huge security team, but even then your team will not have the desired expertise, so they will end up tuning for FPs creating a glaring hole for FNs that hackers will exploit.

What you require is a cloud WAF vendor who handles the complete management of WAF. You need someone who monitors the site 24*7, fine-tune the rules once it is on-boarded based on application need, write new rules based on application need. Many vendors partner with MSSP players to provide the managed part to you, but that again does not work, you need the vendor to do the managed part as they will only know the integrities of the rules written and would know how to fine-tune them without affecting security.

Only the vendor know the updates to WAF, which will affect the overall protection and customization done to a particular site. Disparate service providers without visibility of how vendors are innovating will not be able to provide you an effective solution.

What you need is an effective Managed Cloud WAF vendor. Try AppTrana a completely managed Application security solution that starts with risk detection, identify the risk posture of the application, and fine-tune the WAF rules based on application risk posture and need.

AppTrana provides you

Integrated Risk detection and risk protection, ensuring all the vulnerabilities found in the application are immediately patched in the WAF

WAF is completely managed by the AppTrana team, ensuring there are no FPs without compromising on FNs

Built ground up on the cloud, AppTrana is highly scalable and is built to handle large variance in traffic seamlessly

With AppTrana you will finally get a Cloud WAF. More than 95% of our deployments are in log & mode with a reliability guarantee of 99.99% backed by penalty clauses.

CONCLUSION

Web Application Firewall (WAF) still remains one of the necessary detective or preventive security controls within organizations. Whether you require a WAF to protect your business-critical apps from attacks or comply with industry-standard regulations, choosing the right product plays a vital role. By deploying a robust WAF, you can secure your web apps from attacks like DDoS attacks, SQL injection, and zero-day attacks.

Reference

[1] https://searchsecurity.techtarget.com/feature/The-history-of-the-PCI-DSS-standard-A-visual-timeline

[2] https://www.niscicb.com/PreviousReports

[3] https://ponemonsullivanreport.com/2019/07/the-state-of-web-application-firewalls/

ABOUT INDUSFACE

Indusface is a SaaS company which secures critical Web applications of 2000+ global customers using it's award winning platform that integrates Web application scanner, Web application firewall, CDN and threat information engine. The company has been mentioned in the Gartner Magic Quadrant and Forrester Tech Now report and is CERT-In empanelled as a trusted scanning vendor and is funded by Tata Capital Growth Fund.