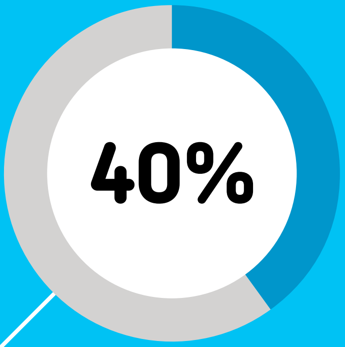
The Top 6 WAF Essentials to Achieve Application Security Efficacy

Introduction

One of the biggest challenges IT and security leaders face today is reducing business risk while ensuring ease of use and employee productivity. The fact is, people need to be able to work whenever and however they need to — meaning any location, device, or network — without being frustrated by an overly constrained or complex user experience.

At the same time, it's essential to protect enterprise apps and data from being compromised by security threats, and ensure full compliance with standards and regulations.

As organizations continue to build and buy web applications, and more of these apps move to the cloud, maintaining a high level of application protection is getting increasingly difficult. The security perimeter is changing and is no longer the edge of the data center. This creates tremendous vulnerabilities to your network and applications, creating a heightened need for protection against a range of cyber threats.



Web app attacks represented 40% of breaches in 2015

WhiteHat Security
Web Applications Security Statistics Report 2016

The solution used to secure web applications and combat these security risks is a web application firewall, or WAF. This eBook will delve into what a WAF is, why it is important, and the six essential features your WAF should have to maintain the highest levels of security efficacy for your organization's application delivery infrastructure.

The Evolution of the Web Application Firewall

Firewalls have significantly improved the overall security posture of organizations since they first came on the scene back in the late 1980s. Developed in the early 1990s, web application firewalls (WAFs) were a new species of firewall initially created to respond to threats beyond the scope of traditional firewalls.

These threats were difficult to defend against because they utilized authorized protocols (such as HTTP), but attacked the application or underlying infrastructure over that protocol. This was especially dangerous because hackers could attack over trusted protocols to directly compromise systems and steal information, effectively bypassing traditional firewall security.

In contrast to regular firewalls, which are designed to restrict access to specific ports, or deny service to unauthorized people, WAFs are much more intelligent. They examine every request and response within the HTTP/HTTPS/SOAP/XML-RPC/Web Service requests to identify attack signatures and abnormal behavior patterns within incoming traffic to a web application.

Simply put, whereas network firewalls defend the perimeter of the network, WAFs sit between the web client and web server, analyzing application-layer traffic for violations in the programmed security policy. This positions the WAF to detect whether an application is not behaving the way it was designed to, and enables you to write specific rules to prevent attacks from reoccurring.

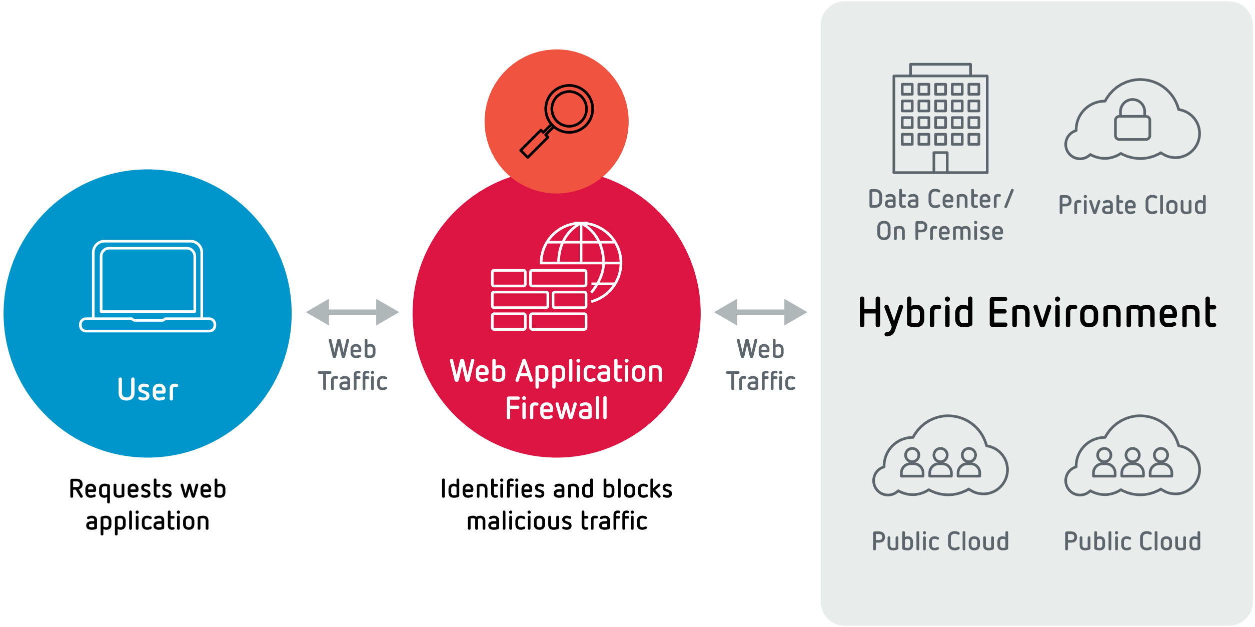
It is also important to differentiate a WAF from a next-generation firewall or NGFW. A WAF is intended to inspect the application traffic on a narrow protocol scope and focus only on that traffic. A NGFW is a comprehensive product to replace or augment existing network firewalls.

Why Web Application Firewalls Are Critical to Security

Every day, thousands of businesses, from the small town bank to the largest enterprise, rely on their web presence to bring in revenue and keep the company moving. WAFs protect this presence by providing essential protection to data and services to help avoid loss of direct revenue, negative impacts to customer confidence, and concerns about sensitive data breaches.

Without WAF security, application vulnerabilities can be exploited to conduct a range of actions — anything from crashing apps, to taking shell control to corrupt databases. In effect, an application compromise can spell big financial and reputational damage to a breached organization.

Because of the nature of web security and how it constantly evolves, it is increasingly difficult to integrate comprehensive security into applications and keep them up-to-date. Having a WAF helps here in two ways: It protects against known threats and it monitors the application layer to identify and protect against new, previously unknown threats.



In short, whether you're conducting business with an online vendor through their web services, or delivering apps to your workforce, WAFs provide the application security you need to dispel risks posed by modern security threats.

Top Six Things to Look for in a Web Application Firewall Solution

When selecting a WAF solution to protect your applications, you should prioritize the following features to achieve application security efficacy.

1 Protection Against The OWASP Top 10

OWASP or "Open Web Applications Security Project," is an open software security community collecting, among other things, the list of top attacks against web servers.

Your WAF must protect web applications and servers from the OWASP Top 10 to ensure security against the most prevalent application attacks.

The effectiveness of a WAF solution's security against the OWASP Top 10 is difficult to discern without testing. Seeking research testing and validation from a trusted organization is a reliable way to gain insight into the effectiveness of leading WAFs in the market.

Consider reviewing the Security Value Map™ (SVM) and Comparative Analysis Report™ (CAR) series by NSS Labs, which evaluates leading WAF products on their ability to prevent intrusions, and detect and mitigate threats.

The OWASP Top 10

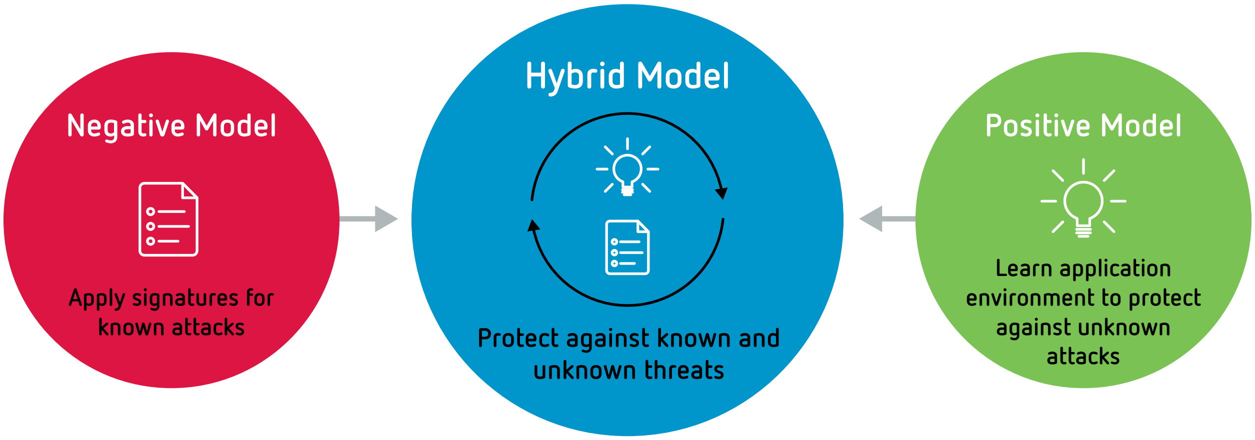
1. Injection
2. Broken Authentication and Session Management
3. Cross-Site Scripting (XSS)
4. Insecure Direct Object References
5. Security Misconfiguration
6. Sensitive Data Exposure
7. Missing Function Level Access Control
8. Cross-Site Request Forgery (CSRF)
9. Using Components with Known Vulnerabilities
10. Unvalidated Redirects and Forwards

2 Protection Against Known and Unknown Attacks

Your WAF should support both a positive and a negative security model.

A negative security model is easy to deploy because it protects against known exploits.

A positive security model denies all transactions by default, but uses rules to allow only those transactions that are known to be valid and safe. This approach is more efficient (fewer rules to process per transaction) and more secure, but it requires very good understanding of the applications being protected.


Negative Model
Apply signatures for known attacks
Hybrid Model
Protect against known and unknown threats
Positive Model
Learn application environment to protect against unknown attacks

3 PCI DSS Compliance

Malicious attacks designed to steal sensitive credit card information are increasing, with more and more security breaches and data thefts occurring daily. PCI DSS requirements have been revised in an attempt to prevent these types of attacks and keep customer data secure.

If your organization works with, processes, or stores sensitive credit card information, you must comply with PCI DSS requirements. You must strengthen your security posture by protecting your critical web applications, which are often easy pathways for malicious attackers to gain access to sensitive cardholder data.

While you can adhere to PCI DSS standards by deploying a vulnerability scanner or a WAF, the most effective solution is to integrate the data from scanning technology with the attack-mitigation power of a WAF.

The WAF you invest in should identify, isolate, and block sophisticated attacks without impacting legitimate application transactions. In addition, your WAF should offer PCI reporting, which determines if compliance regulations are being met, and if they are not, details the steps required to become compliant.

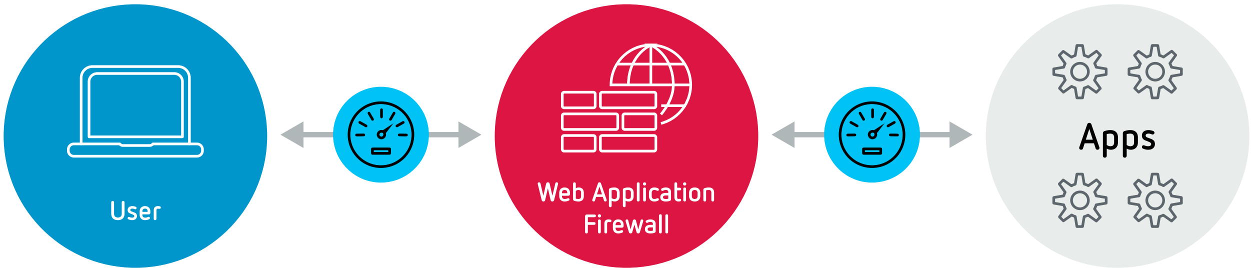
> **"Of all the data breaches investigated over the last ten years, not a single company has been found to be PCI compliant at the time of the breach."**
>
> **Verizon**
> 2015 PCI Compliance Report

4 High Performance Without Negative Impact

Performance is key when it comes to a WAF. The WAF you choose should not impact the performance of existing infrastructures, including application and network devices.

This means that even though the WAF acts as the security proxy to the application, the application continues to transact the data without suffering from a backlog of requests and does not collapse under heavy loads.

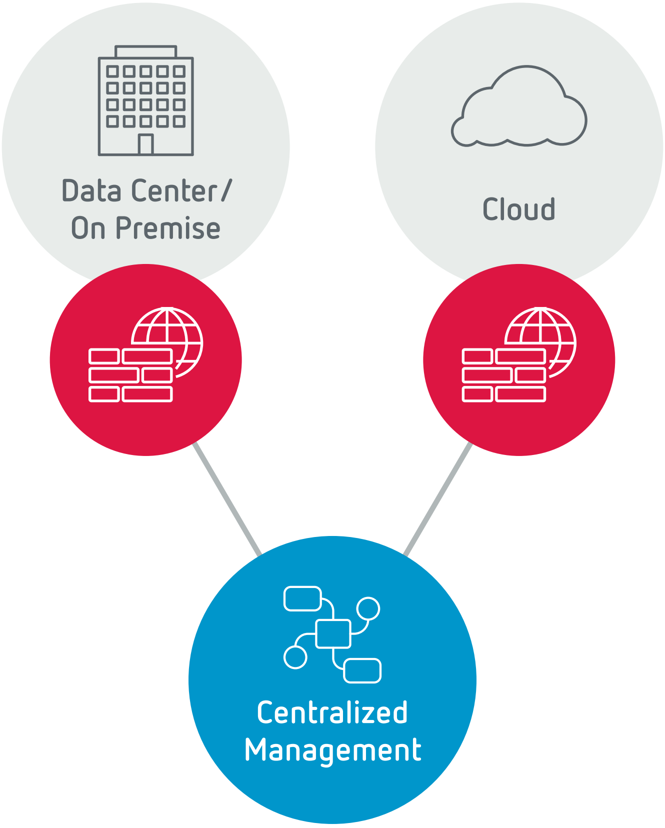
The application should behave as though no WAF is present. And from the end user perspective, the WAF should be completely transparent. Users should not experience any noticeable delay or hindrance of service.



5 Centralized Management

Centralized management is crucial when you're dealing with web application infrastructure that is distributed in different environments, and especially across the globe.

You want to be able to manage different WAF appliances without needing to connect to each appliance separately. This means your WAF solution needs to integrate with a Centrallized Management platform, allowing you to build, maintain, and enforce a unified security policy across your entire organization.



6 Application Vulnerability Prevention

Web application vulnerabilities are among the most common causes of data breaches. Vulnerabilities — unique to each application — leave companies' web infrastructures exposed to attacks such as cross-site scripting, SQL injections, cookie poisoning, and others.

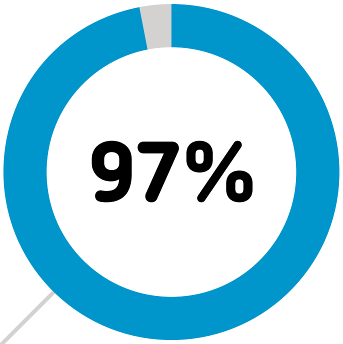
When defects and vulnerabilities are found in software code, your WAF should rapidly apply fixes (virtual patches) to prevent exploitation by an attacker.

This virtual patching requires no immediate changes to the software, and it allows organizations to secure applications immediately — and in some cases, automatically — upon dynamic application testing. Virtual patches are a key component of a strong WAF, often requiring integration with a vulnerability scanner.

In addition, your WAF solution should integrate with points such as security information event management systems (SIEM), log retention systems, identity management, incident management, and application scanners to provide layered and automated security.

"97% of applications tested by Trustwave in 2015 contain at least one vulnerability."

2016 Trustwave Global Security Report



Meet NetScaler AppFirewall: The Industry Leading WAF that Integrates with NetScaler ADC to Ensure Application Security Efficacy

NetScaler AppFirewall is a comprehensive full function ICSA, Common Criteria, FIPS-certified web application firewall that analyzes all bi-directional traffic, including SSL-encrypted communication, to protect against a broad range of security threats without any modifications to applications.

It offers protection from a number of different known and unknown threats and has the ability to perform deep-packet inspection of HTTP, HTTPS, and XML as well as protection against the OWASP Top 10.

NetScaler AppFirewall is available both as a standalone appliance and as a WAF solution tightly integrated into the NetScaler ADC platform, and is available across its various form factors including physical, virtual, and containerized. This gives you the flexibility to deploy different form factors based on different needs

NetScaler standalone AppFirewall provides the highest throughput in the industry at 44 Gbps, and according to NSS Labs, NetScaler AppFirewall is the recommended leader in the WAF market today with the best price to performance ratio.

NetScaler AppFirewall can be used in conjunction with NetScaler Security Insight — a powerful security management, reporting, and analytics solution that is part of NetScaler Management and Analytics System — to provide an overall view of security posture, a summary of factors contributing to the level of threat imposed on applications, and actionable data that security teams can use to mitigate security risks, maintain integrity, and achieve compliance.

Citrix NetScaler AppFirewall is the only WAF that gives you the performance and essential features you need, so you can say yes to digital transformation and application security efficacy.

Learn more about Citrix NetScaler AppFirewall

www.citrix.com/products/netscaler-appfirewall