
# Delivering best-in-class web application security to the modern enterprise

Understand the current web application threat landscape, learn why traditional network security solutions fail to provide a complete protection against today's emerging threats and why your organization needs a web application firewall to mitigate IT risks.



+91 120 4545911 | info@haltdos.com | www.haltdos.com

# Introduction

This document details the current web application challenges, web application protection problem, most common attacks on the web applications and choosing Web Application Firewall over a Traditional Firewall. It also explains why a web application firewall is an essential component of any organization's web security strategy and how HaltDos WAF - with its unique and comprehensive offering of web application security, DDoS protection and Load Balancing capabilities – is the ideal solution for meeting this need.

# Web Application Firewall - An Overview

## Current Challenges

Cyber-criminals are targeting web applications from all around the world in their most upstream form, costing businesses and organizations a lot of money and a significant risk to their brand reputation. Factors such as the rapid adoption of cloud computing, continued growth of web application traffic, use of open source technologies, security vulnerabilities, complexity of web applications and an increase in the overall sophistication multi-layer attacks has led to an extremely challenging environment for an organizaiton's IT security.

Recent cyber attacks on critical IT infrastructure demonstrates the urgent need for improved cybersecurity practices and measures. As the cyber threats grow, so must our abilities to neutralize them.

## The web application protection problem

There are numerous reasons why online resources represent a substantial risk to today's organizations. The most prominant ones are the expansion of these resources, the fact that they are being continuously targeted by today's cyber attackers and are protected by some deficient so-called "application security" solution.

**Growing web resources accoss organizations:**

Today's organizations are continuously relying on building and outsourcing web - applications for staying ahead of the competition and to access, collect, process, and relay sensitive data to execute business logic. While these web applications are being used by an organization's external as well as internal users, the corresponding protections are needed at more than just the network perimeter to take care of their security.

## What makes an web application a target?:

Different web applications deployed at an organization have completely different functions and purposes, but all applications can be a target for hackers.

So, what basically makes an application a target?

**Popularity** – If an organization have a popular website that is getting a good number of visits every minute and probably have many competitors too. So, with respect to the business point to view, any damage to their brand can facilitate their competitors. Attacks on popular websites conjointly tend to be more news-worthy if the attacker is looking for "bragging rights."

**Protest/Politics** – Groups like Anonymous orchestrate attacks on government, non secular and corporate website applications just for fun or to form a statement.

**Disgruntled employees** – Not all attacks come from the outside, often times attacks are orchestrated or assisted with the help of somebody from an organization itself.

Today's hackers and nation states are increasingly targeting websites in an attempt to gain illicit access to enterprise networks and highly valuable digital assets. Since Web applications present a number of unique security challenges that require purpose-built security solutions, high profile cyber attacks have stimulated the demand for Web Application Firewall (WAF) systems.

## Deficient web application protection solutions:

The Web Application Firewalls (WAFs) are designed to minimize the business risks and protect company's Web applications against various critical cyber attacks.

Let's take a look at Yahoo's data leak in 2013 where 1 billion user accounts were compromised or the more recent Equifax data leak which affected its 143 million customers, these events show the increased risk each web application is facing. And such high-profile data breaches are driving organizations to proactively evaluate WAF solutions as a means to minimize business risk from unprotected Web applications.

While most of the organizations are already deploying sheer diversity of web application protection solutions which require high-level technical expertise and manual intervention for attacks, some of them are still hesitant to deploy WAF fearing that they lack the time, expertise and budgets necessary.

On the other hand, to prevent and mitigate threats in real-time, a Web Application Firewall includes countless number of security rules on the basis of well-known attack signatures as well as rules specific to each application. This means that the WAF configuration need periodic updates to include new attack signatures in order to stay effective.

In most organizations, this activity is performed by an experienced security team on a regular basis. While performing these security audits in a timely fashion is an expensive and time-consuming task. It also means that security teams should have in-depth knowledge of all the web applications they are securing.

Another issue for updating security policies in a timely fashion is the occurrence of "false positives." This happens when a genuine user or request gets denied by the WAF because it triggers a rule and gets classified as an attack. False positives can occur due to a new policy change targeting a newly found attack. It can also happen if security policies and rules don't closely follow application demands. False positives are a big operational challenge for teams managing web application security. Since such events affect business and customer experience, it's not surprising that teams prioritize avoiding false positives over application security.

Also, there are many other issues with existing WAF solutions, such as deployment options, real-time visibility, Access control, protection against DDoS attacks, periodic reporting, etc. but the key takeaway is that they can be very much costly for an average-sized organization.

## What are the 4 most common attacks on web applications?

Hackers have a lot of choices for attack vectors to bring down an organization's online resources, but here is a list of some of the most common types of web application attacks on businesses:

**1) SQL Injection -** Hackers carry out SQL injection attacks to gain access to the database, spoof a user's identity, and destroy or alter data in the database of an organization. SQL injection happens when malicious SQL statements are inserted into form fields to try and gather information from the database. This information allows the hacker to access, modify or destroy information in the database. With SQL injection, a hacker can change the price of a product, and gain client information such as credit cards numbers, passwords and contact information.

**2) Cross-Site Scripting (XSS) -** Hackers use Cross-Site Scripting (XSS) attacks to have browsers execute their malicious payloads to deface an organization's website to promote their brand or their hacktivist ideals . XSS occurs when malicious code is injected into an application that executes on the client side.

**3) Distributed Denial of Service (DDoS) attacks -** To make a website / web application temporarily unavailable, hackers launch Distributed Denial of Service (DDoS) attacks through easily available DDoS tools or by forming a botnet of multiple infected machines and use it to launch flood attacks.

.

DDoS attacks generate requests from thousands of IP addresses in an attempt to flood the internet pipe/website with large volume of illegitimate traffic, making it impossible for the server to respond to user's legitimate requests. DDoS attacks or bots can slow a site down or make it temporarily unavailable.

**4) Cross-Site Request Forgery (CSRF) -** Attackers hijack trusted user sessions to make unwanted purchases on behalf of users with Cross Site Request Forgery (CSRF) attacks. CSRF attacks occur when a user is tricked into clicking a link or downloading an image that executes unwanted or unknown actions on an authenticated user session.

## Choosing a Web Application Firewall over Traditional Firewall

Commonly deployed security solutions clearly have a role to defend organization's business- critical web applications. Hence, It is important to understand their limitations for providing an adequate level of protection.

Traditional firewalls protect IT environments against external attacks, by allowing and blocking connections to certain areas. These firewalls control incoming as well as outgoing network traffic based on a set of rules.

Here is a basic example:

Let's suppose an organization has a web server inside its network infrastructure. In order for the web server to be reachable from outside the organization, some rules will have to be established to authorize web traffic to and from that server. Therefore, Some "ports" will be open, on a given IP address of the organization's server). But allowing web traffic only does not guarantee that this traffic is legitimate. The web has enabled many possibilities and allowed easy access to resources and data. Unfortunately, web technologies are not completely safe by nature and threats are as numerous as opportunities. Traditional firewalls cannot analyze in details what is reaching the server.


*Figure1 : Traditional Firewall - Bad traffic coming in*

By opening communication channels to web servers, the door also gets open for the attackers to launch targeted cyber attacks such as application layer attacks.

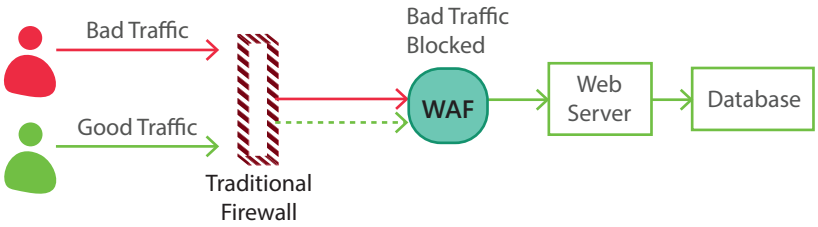



*Figure 2 : Web Application Firewall blocking Bad traffic*

As the web traffic can embed many types of attacks such as SQL injections, Cross-Site Scripting (XSS) , Cross Site Request Forgery (CSRF), Session hijacking attack, etc. With the help of a Web Application Firewall solution an organization can protect their vulnerable resources against such attacks.

## HaltDos WAF

Its an unique and comprehensive web application firewall solution which intelligently fits into an organization's security architecture and elevate the importance of selecting a full-featured solution.

HaltDos' Web Application Firewall (WAF) uses state of the art anomaly detection techniques to protect online web applications from common and zero-day web exploits, SQL injections, cross-site scripting (XSS), CSRF, OWASP top 10 vulnerabilities and also the application layer attacks that affect application availability or compromise the security of your web services.

Beyond handling common web application threats, HaltDos WAF is fully-integrated with advanced DDoS protection which is capable to detect and mitigate complex types of DDoS attacks on the web applications in real time, not just that HaltDos WAF has an in-built load balancing features for improving the performance and reliability of websites, applications, databases and other services.

HaltDos customers also get an unified monitoring when an attack occurs, including the type and size of the attack, IP origin, Attack vectors, mitigation process & access logs. It also identifies the false positives in real time and protect resources without

any human intervention.

Where traditional WAFs look at individual transactions through an cumbersome operation, HaltDos WAF allows deep visibility and 360 degree protection to its users with a centralized management for WAF, DDoS protection and Load Balancing.

## Key Highlights:

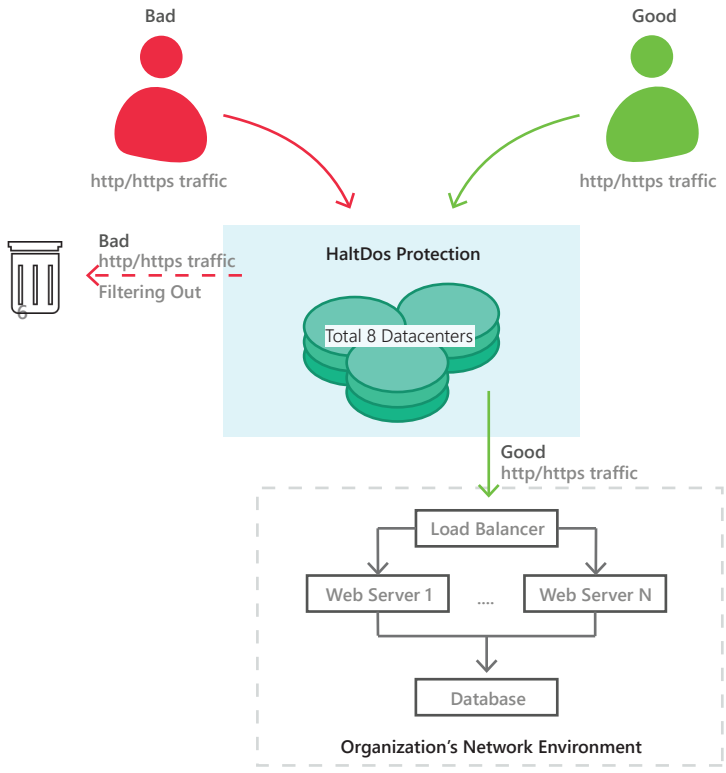
**High Performance:** Low latency and high mitigation capacity for very high volume and sophisticated attacks and maintains excellent user response time even when under attack.

**Multi-Layered Solution:** HaltDos combines network behavioral analysis (NBA), heuristic and reputation techniques to detect bot traffic from legitimate user traffic.

**Unified Monitoring:** Per-user customization of real-time dashboards and historical records of attack trends and network patterns

**Maintains Business Operations:** Full protection against emerging network threats and maintain network performance even when under high volume network attacks.

## Holistic Network Diagram (HaltDos WAF)



## Conclusion

This is an undeniable fact that the cyber-attacks are growing with new introductions of emerging and more advanced security threats, and to fight against them, ordinary network firewalls fail to provide an adequate protection for the handful of web applications that an average organization deems important. To thoroughly protect their organization's diversity of internet-facing web applications, security teams needed to implement a fully managed solution that provides a comprehensive security to these web applications against the network layer attacks as well as application-layer attacks. This resulted in WAF integrating with other solutions as advanced Distributed Denial of Service (DDoS) protection with load balancing capabilities. A full-featured WAFs such as HaltDos WAF deliver a degree of threat protection that uses state of the art anomaly detection techniques to block application layer attacks with zero false positives and also provides a fine-grained configuration and application server level monitoring that provides full spectrum visibility with no single point of failure.

## Office Address

E-52, Sector - 3, Noida,
Uttar Pradesh - 201301
Ph: +91 120 4545911
Fax: +91 120 4243669
Email: info@haltdos.com

## About HaltDos™

haltDos is an AI driven website protection service that secures online businesses against today's cyber threats. It offers comprehensive yet affordable Web Application Firewall, DDoS protection and Load Balancing features in a single platform which allows business to secure their web applications with zero-management. haltDos customers gain full-spectrum visibility of their network with high-end WAF & Anti-DDoS solution which is capable of handling complex cyberattacks with zero false positives. haltDos solutions are in use globally.

To Learn more visit at www.haltdos.com