

Web Application Firewall

As businesses become almost entirely reliant on data in their day-to-day operations, customer relationships and marketing campaigns, how businesses protect their critical data and applications has become an increasing priority.

Due to the volume of data now stored on company servers, organisations have become lucrative targets for cybercrime, with hackers and malicious actors utilising a range of methods to exploit weaknesses and gain access to critical information. So what can you do to provide an extra layer of protection? A web application firewall is a good place to start.

What is a web application firewall?

A web application firewall (WAF) differs from a standard firewall as it is specifically configured to protect web applications and websites, specifically code, whereas standard firewalls work based on access controls.

A WAF sits directly in front of the application layer of a web server and examines every HTTP/HTTPS request that comes through as they pass to and from the firewall and web servers. By applying a set of specific configured rules as outlined by the user, any illegitimate traffic will be filtered out. This can consistently be adapted in line with new threats posed to the application or website.



How does a Web Application Firewall work?

A WAF will protect your web apps by filtering, monitoring, and blocking any malicious traffic travelling to the application or website. It does this by adhering to a set of rules outlined by the user that will help determine the difference between valid and malicious traffic. Acting similarly to a proxy server, a WAF acts as the intermediary between the app and a malicious user.

WAFs can come in several forms depending on the application or the size of the application and this can come in the form of software, appliance or a specialised 'as-a-service' model, all of which require a set of rules outlined by the user. Although nearly all WAFs will require you to update your rules, advances in machine learning enable some to update automatically.



Our web application firewall service

At Hyve, security is at the forefront of everything we do. With this in mind, we offer an enterprise-grade, cloud-based web application firewall, built specifically for your business and fine-tuned by our team of experts. Our highly available WAF provides your web application with the extra layer of protection you need, helping you to block any attacks from HTTP/HTTPS traffic such as cross-site scripting or SQL injection. As cybersecurity threats evolve, our team of security experts will help

you review the rules in place and advise where necessary to further secure your platform.

We work with industry-leading projects such as ModSecurity and Alert Logic to provide our WAF service at a cost-effective price point for a wide range of businesses.

