

Web Application Firewall (WAF)

Learn how Web Application Firewalls defend your web apps from common attacks

What is a web application firewall?

A web application firewall (WAF) helps protect a company's web applications by inspecting and filtering traffic between each web application and the internet. A WAF can help defend web applications from attacks such as cross-site request forgery (CSRF), cross-site-scripting (XSS), file inclusion, and SQL injection ([/web/20210410115503/https://www.rapid7.com/fundamentals/web-application-vulnerabilities/](https://www.rapid7.com/fundamentals/web-application-vulnerabilities/)).

A WAF can be especially beneficial to a company that provides an e-commerce site, online financial services, or any other type of web-based product or service involving interactions with customers or business partners. In these cases, WAFs can be especially useful in preventing fraud and data theft. However, since a WAF is not designed to ward off all types of attacks, it works best as part of a suite of tools that support a [comprehensive application security program](#) ([/web/20210410115503/https://www.rapid7.com/solutions/application-security/](https://www.rapid7.com/solutions/application-security/)).

FUNDAMENTALS

Web Application Security

Select Section

Web Application Security
and Scanning: Explanation
and Deep Dive
(/web/20210410115503/https://www.rapid7.com/fundamentals/web-application-security/)

Web Application Security
Testing
(/web/20210410115503/https://www.rapid7.com/fundamentals/web-application-security-testing/)

Web Application Vulnerabilities
(/web/20210410115503/https://www.rapid7.com/fundamentals/web-application-vulnerabilities/)

Key benefits of a WAF

A WAF can provide critical protection for any online business that must securely handle private customer data. Businesses typically deploy a WAF to shield their web applications from sophisticated and targeted attacks, like [cross-site scripting \(XSS\)](#). [\(/web/20210410115503/https://www.rapid7.com/fundamentals/cross-site-scripting/\)](#) and [SQL injection](#). [\(/web/20210410115503/https://www.rapid7.com/fundamentals/sql-injection-attacks/\)](#), that might result in fraud or data theft. When successful, these types of incursions can severely compromise customer confidence and even result in regulatory penalties. The added protection that a WAF provides can help safeguard a company's reputation and position in the market.

[Application Security Testing Programs](https://www.rapid7.com/fundamentals/application-security-testing-programs/)
(/web/20210410115503/https://www.rapid7.com/fundamentals/application-security-testing-programs/)

[DevSecOps: Definition and Deep Dive](https://www.rapid7.com/fundamentals/devsecops/)
(/web/20210410115503/https://www.rapid7.com/fundamentals/devsecops/)

[Dynamic Application Security Testing \(DAST\)](https://www.rapid7.com/fundamentals/dast/)
(/web/20210410115503/https://www.rapid7.com/fundamentals/dast/)

[Software Development Life Cycle \(SDLC\)](https://www.rapid7.com/fundamentals/software-development-life-cycle-sdlc/)
(/web/20210410115503/https://www.rapid7.com/fundamentals/software-development-life-cycle-sdlc/)

[Web Application Firewall \(WAF\)](https://www.rapid7.com/fundamentals/web-application-firewalls/)
(/web/20210410115503/https://www.rapid7.com/fundamentals/web-application-firewalls/)

[Runtime Application Self-Protection \(RASP\)](https://www.rapid7.com/fundamentals/runtime-application-self-protection/)
(/web/20210410115503/https://www.rapid7.com/fundamentals/runtime-application-self-protection/)

[Cross-Site Request Forgery \(CSRF, XSRF\)](https://www.rapid7.com/fundamentals/cross-site-request-forgery/)
(/web/20210410115503/https://www.rapid7.com/fundamentals/cross-site-request-forgery/)

[Continuous Integration and Continuous Delivery or Continuous Deployment \(CI/CD\)](https://www.rapid7.com/fundamentals/cicd/)
(/web/20210410115503/https://www.rapid7.com/fundamentals/cicd/)

A WAF also lightens the administrative burden of ensuring proper [web application security testing](https://www.rapid7.com/fundamentals/web-application-security-testing/) (/web/20210410115503/https://www.rapid7.com/fundamentals/web-application-security-testing/) on a continual basis. By helping to proactively set guidelines and rules, application security teams are able to monitor for what should and shouldn't be allowed through a WAF. From there, teams can receive timely notification of an attack in progress so they can respond much more rapidly to potential security incidents.

Because a WAF provides security administrators with the application visibility necessary to demonstrate compliance with regulatory standards like PCI, HIPAA, and GDPR, it can be valuable from a compliance perspective as well. Combined, all of these advantages can help a company strengthen its web application security and better safeguard customer data from evolving threats.

Stateless WAFs vs. stateful WAFs

A WAF sits between a company's web applications and the requests coming in from the internet. Via reverse proxy, it monitors, filters, or blocks data packets as they travel to and from a web application. In doing so, it attempts to screen out potentially harmful traffic that may enable web exploits. A WAF may come in the form of a cloud-based solution, an appliance, a server plugin, or a filter.

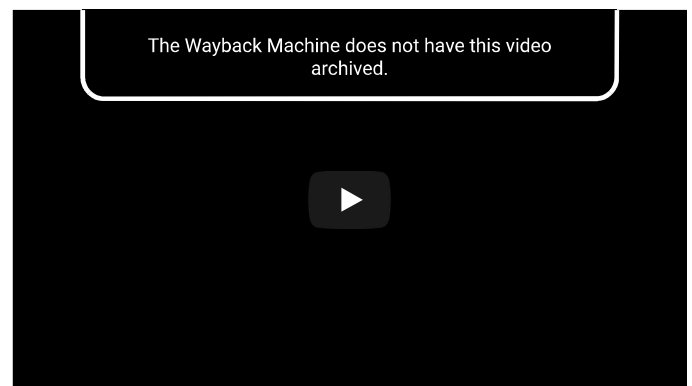
Early WAFs, which are known as stateless WAFs, used static rules to analyze potential threats arriving via inbound requests to a company's web application servers. Using pattern recognition, they effectively generated educated guesses on how a web application might react to a specific form of attack using predetermined models of application behavior and attack behavior. For example, stateless WAFs might check how quickly requests were coming in, whether they were originating from the same source, and other behavioral metrics that might indicate malicious activity was underway.

Stateless WAFs could perform such tasks much more rapidly than their human counterparts, but they were not adaptable or nimble enough to successfully ward off evolving attacks. A continual game of cat and mouse ensued in which attackers, upon discovering that their initial form of attack on a web application had been unsuccessful, would simply devise a new form of attack behavior that the WAF had not seen before and could not prevent. Then, when the WAF eventually received new rules that could ward off this new attack variant, the attackers would come up with yet another method for evading detection.

The second generation of WAFs, known as stateful WAFs, offers more agile defenses than its predecessor. Stateful WAFs can enrich collected data with relevant context and analyze a web application's current threat landscape. Since they take a broader, more contextual view into account, stateful WAFs are better at detecting critical issues such as DDoS attacks and "low and slow" attacks that attempt to undermine security by flying under the radar.

Another technology used for monitoring and protection is [Runtime Application Self-Protection \(RASP\)](https://www.rapid7.com/fundamentals/runtime-application-self-protection/). [\(/web/20210410115503/https://www.rapid7.com/fundamentals/runtime-application-self-protection/\)](https://www.rapid7.com/fundamentals/runtime-application-self-protection/). RASP blocks malicious traffic without the need for static rules using the application itself. Rather than relying on predictions about how an application might behave in a particular scenario, RASP assesses actual application behavior to detect potentially malicious activity (for example, a call to a database, a request to open a file, or a request to start a shell for the purposes of executing a command) as it occurs.

This can cut down on false positives often seen when using a WAF, giving a security team more accurate insight into potential attacks in real time. And, since it uses the application itself, RASP can still assess an application's security even as the application is continually updated and further developed. RASP fits more easily into a continuous process because you can watch how the app behaves as you continually push code changes instead of having to manipulate the static rules for WAF. WAF and RASP can complement one another, combining forces to provide a business with comprehensive and robust application security.



3 tips for success with a WAF

Here are three tips to ensure that your business successfully maximizes the benefits of a WAF:

1. Make sure your WAF supports your application security objectives

There are many WAF solutions available, each with varying security features and techniques for both identifying and preventing attacks. Make sure that any WAF you choose supports your specific application security objectives.

2. Carefully evaluate and test your WAF solution

In order to truly understand how a WAF can serve as an integral part of your application security program, it may be beneficial to test any WAF solution you are evaluating before making a final decision on whether to implement it. That way, you can assess and understand how it will function in coordination with other application security tools you may be using, such as RASP, since these technologies are not mutually exclusive and can be used in tandem for the most comprehensive coverage.

3. Consider what in-house resources you will need

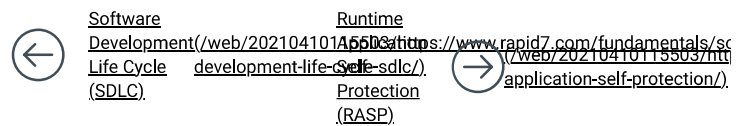
While you're evaluating a WAF solution, think about what in-house resources you will need to make the most of it. You may determine that you will need to build additional skills and capabilities within the security team, for example, or you may want to consider how implementing a WAF will change existing security processes your team has in place.

Businesses face increasingly sophisticated attacks on their web applications as malicious actors seek a payday from fraud and data theft. Ensuring proper web application security has never been more critical, but companies can make significant strides toward protecting their web applications and customer data by adopting a web application firewall. It's an essential part of a robust application security toolkit as well as a modern application security program.

Do I need a Web Application Firewall (WAF)?

With cyberattacks becoming increasingly more complex, businesses and organizations must put themselves in the best position to defend themselves and their clients from malicious intent. Companies involved in e-commerce, online financial services, and various other web-based products face a constant threat of fraud and data theft, which leaves them prone to compromised customer trust and possible regulatory disciplines.

Alongside a suite of tools, WAFs can add an essential extra layer of defense to an already-robust application security program. Security professionals can leverage a web application firewall to monitor a possible attack-in-progress by receiving alerts for activity which violates pre-determined guidelines and rules. This visibility ensures that security teams have the necessary capacity to fulfill regulatory standards, while still maintaining the utmost protection for customer data.



Search all the things

[BACK TO TOP](#)

[./\(web/20210410115503/https://www.rapid7.com/\).](https://web.archive.org/web/20210410115503/https://www.rapid7.com/)

CUSTOMER SUPPORT

[+1-866-390-8113 \(Toll Free\)](https://web.archive.org/web/20210410115503/tel:1-866-390-8113) [./\(https://web.archive.org/web/20210410115503/tel:1-866-390-8113\)](https://web.archive.org/web/20210410115503/tel:1-866-390-8113)

SALES SUPPORT

[+1-866-772-7437 \(Toll Free\)](https://web.archive.org/web/20210410115503/tel:866-772-7437) [./\(https://web.archive.org/web/20210410115503/tel:866-772-7437\)](https://web.archive.org/web/20210410115503/tel:866-772-7437)

Need immediate help with a breach?



[CONTACT US](#)

SOLUTIONS

[All Solutions \(https://web.archive.org/web/20210410115503/https://www.rapid7.com/solutions\)](https://web.archive.org/web/20210410115503/https://www.rapid7.com/solutions)

[Industry Solutions \(https://web.archive.org/web/20210410115503/https://www.rapid7.com/solutions/industry\)](https://web.archive.org/web/20210410115503/https://www.rapid7.com/solutions/industry)

[Compliance Solutions \(https://web.archive.org/web/20210410115503/https://www.rapid7.com/solutions/compliance/\)](https://web.archive.org/web/20210410115503/https://www.rapid7.com/solutions/compliance/)

SUPPORT & RESOURCES

[Product Support \(https://web.archive.org/web/20210410115503/https://www.rapid7.com/for-customers\)](https://web.archive.org/web/20210410115503/https://www.rapid7.com/for-customers)

[Resource Library \(https://web.archive.org/web/20210410115503/https://www.rapid7.com/resources\)](https://web.archive.org/web/20210410115503/https://www.rapid7.com/resources)

[Customer Stories \(https://web.archive.org/web/20210410115503/https://www.rapid7.com/about/customers\)](https://web.archive.org/web/20210410115503/https://www.rapid7.com/about/customers)

[Events & Webcasts \(https://web.archive.org/web/20210410115503/https://www.rapid7.com/about/events-webcasts\)](https://web.archive.org/web/20210410115503/https://www.rapid7.com/about/events-webcasts)

[Training & Certification \(https://web.archive.org/web/20210410115503/https://www.rapid7.com/services/training-certification\)](https://web.archive.org/web/20210410115503/https://www.rapid7.com/services/training-certification)

[IT & Security Fundamentals \(https://web.archive.org/web/20210410115503/https://www.rapid7.com/fundamentals\)](https://web.archive.org/web/20210410115503/https://www.rapid7.com/fundamentals)

[Vulnerability & Exploit Database \(https://web.archive.org/web/20210410115503/https://www.rapid7.com/db\)](https://web.archive.org/web/20210410115503/https://www.rapid7.com/db)

ABOUT US

[About \(https://web.archive.org/web/20210410115503/https://www.rapid7.com/about\)](https://web.archive.org/web/20210410115503/https://www.rapid7.com/about)

[Company \(https://web.archive.org/web/20210410115503/https://www.rapid7.com/about/company\)](https://web.archive.org/web/20210410115503/https://www.rapid7.com/about/company)

[Leadership \(https://web.archive.org/web/20210410115503/https://www.rapid7.com/about/leadership\)](https://web.archive.org/web/20210410115503/https://www.rapid7.com/about/leadership)

[News & Press Releases \(https://web.archive.org/web/20210410115503/https://www.rapid7.com/about/news\)](https://web.archive.org/web/20210410115503/https://www.rapid7.com/about/news)

[Customers \(https://web.archive.org/web/20210410115503/https://www.rapid7.com/about/customers\)](https://web.archive.org/web/20210410115503/https://www.rapid7.com/about/customers)

[Public Policy \(https://web.archive.org/web/20210410115503/https://www.rapid7.com/about/public-policy\)](https://web.archive.org/web/20210410115503/https://www.rapid7.com/about/public-policy)

[Investors \(https://web.archive.org/web/20210410115503/https://investors.rapid7.com/\)](https://web.archive.org/web/20210410115503/https://investors.rapid7.com/)

CONNECT WITH US

[Contact \(https://web.archive.org/web/20210410115503/https://www.rapid7.com/contact\)](https://web.archive.org/web/20210410115503/https://www.rapid7.com/contact)

[Blog \(https://web.archive.org/web/20210410115503/https://blog.rapid7.com/\)](https://web.archive.org/web/20210410115503/https://blog.rapid7.com/)

[Support Login \(https://web.archive.org/web/20210410115503/https://support.rapid7.com/\)](https://web.archive.org/web/20210410115503/https://support.rapid7.com/)

[Careers \(https://web.archive.org/web/20210410115503/https://www.rapid7.com/careers\)](https://web.archive.org/web/20210410115503/https://www.rapid7.com/careers)

[Rapid7 \(https://web.archive.org/web/20210410115503/https://www.rapid7.com/rapid7\)](https://web.archive.org/web/20210410115503/https://www.rapid7.com/rapid7)

© Rapid7 [Legal Terms \(https://web.archive.org/web/20210410115503/https://www.rapid7.com/legal\)](https://web.archive.org/web/20210410115503/https://www.rapid7.com/legal) |

[Privacy Policy \(https://web.archive.org/web/20210410115503/https://www.rapid7.com/privacy-policy\)](https://web.archive.org/web/20210410115503/https://www.rapid7.com/privacy-policy) |

[Export Notice \(https://web.archive.org/web/20210410115503/https://www.rapid7.com/export-notice\)](https://web.archive.org/web/20210410115503/https://www.rapid7.com/export-notice) |

[Trust \(https://web.archive.org/web/20210410115503/https://www.rapid7.com/trust\)](https://web.archive.org/web/20210410115503/https://www.rapid7.com/trust)