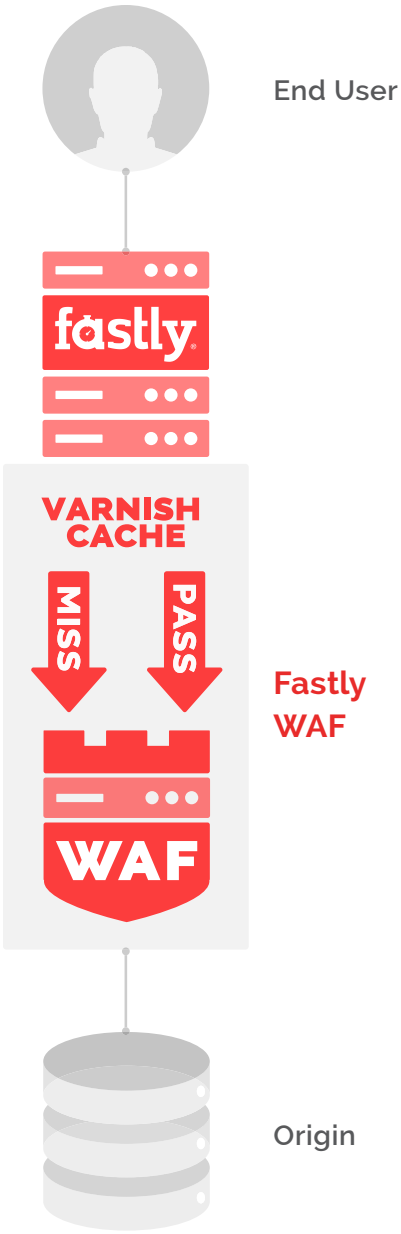
fastly

Fastly WAF

Always on, world-class application-layer protection

In 2016, 40% of web application threats led to breaches — a fivefold increase from the previous year. As the scope and complexity of application layer attacks grow, a web application firewall (WAF) is critical to protecting your web applications. Yet the marketplace is crowded with expensive on-premise solutions and inconsistent cloud-based services. If you choose an on-premise solution, you are locked into the cycle of purchasing, maintaining, and updating equipment. If you select a cloud solution, you may do so at the expense of poor user experiences caused by outages or increased latency.

Protecting your web applications is crucial. And maintaining an optimal experience to your customers is critical to the success of your business. How do you accomplish both?



Why Fastly?

Fastly's WAF eliminates the tradeoff between security and high-quality performance; customers benefit from complete control and real-time visibility, without the latency issues associated with many WAFs.

Because Fastly's WAF analyzes, filters, and blocks only origin-bound traffic attempting to refresh the cache, most attack traffic is stopped at the Fastly cache, protecting your origin traffic from malicious attacks while providing a great user experience for your customers.

Fastly's PCI DSS compliant network delivers powerful edge enforcement for faster protection against the latest-known web application vulnerabilities, DDoS, and botnet attacks. We provide real-time insights into security events and notifications, instant rule changes, and the ability to update security policies across the globe in milliseconds.

Comprehensive 24/7/365 protection

Fastly's cloud-based WAF uses third-party rules from the OWASP Core Rule Set, commercial sources, and the Fastly application security research team who track application-level and network threats.

Customers are protected from: injection attacks and malicious inputs, cross site scripting, data exfiltration, HTTP protocol violations, and other OWASP top 10 Threats.

Always on — you are protected from constantly growing list of known threats around the clock.

For a **complete security solution**, WAF can be used with Fastly's DDoS (Layer 3, 4, and 7 protection) and Bot Detection and mitigation services.

sales@fastly.com | fastly.com

Superior performance

Our WAF is fully integrated into our Varnish-based edge cloud platform. By processing only origin traffic, Fastly's WAF preserves cache performance. Integration with our edge cloud platform also extends support for IPv6 and HTTP/2.

Very low performance hit: 1.5-20ms for origin bound traffic (depending on payload size and rules).

Deeper integration

Third-party CMS platforms increasingly become the target for application-layer attacks. The ability to virtually patch these platforms allows you to protect your applications until you roll out software updates. We apply pre-defined rulesets to protect known vulnerabilities in popular platforms like Drupal and WordPress. You can also quickly add, remove, or change WAF-based rules for these platforms.

Build complex apps on our platform, using Varnish Configuration Language (VCL) to push application logic to the edge.

No black boxes. You have complete control

You get access to real-time logs and the ability to make configuration changes on the fly. Fastly's WAF gives you access to 100% of your logs with a mere one-to-two second delay. Quickly identify potential application-layer threats and make instant configuration changes to your WAF rules within our service. Real-time log streaming also gives you immediate visibility into the impact of attack mitigation efforts. We also keep a history of previous configurations so you can quickly roll back if needed.

Real-time access to WAF events and notifications from the edge. You have full visibility into attack traffic and rule configuration

Real-time configuration changes to WAF rules from within our service using the Fastly API.

Fastly will monitor and analyze your traffic, tune the WAF settings, and **hand control over to you.** You can make policy changes and see in near-real time those changes in action against the attack traffic.

Fastly WAF specifications & features

- **One, PCI compliant network**
- **Save money: only pay for WAF-inspected traffic, not all traffic**
- **You have control: real-time log streaming empower you to mitigate attacks as they happen**
- **Instant worldwide security policy changes using the Fastly API**