fastly

Powered by Signal Sciences

PRODUCT DATASHEET

Fastly Next-Gen WAF

Protect your apps and APIs everywhere from a single solution

When your business is growing and innovating at a rapid rate, other web application firewalls can fail to keep up: too many false positives, limited DevOps integrations, and incompatibility with your mix of applications and differing architectures. The Fastly Next-Gen WAF (powered by Signal Sciences) provides advanced web application and API protection (WAAP) for your applications, APIs, and microservices, wherever they live, from a single unified solution.

Protection everywhere your apps operate

Fastly's next-gen WAF flexibly deploys in any environment and can protect apps and APIs wherever they are—in containers, on-prem, in the cloud, or on the edge—with one integrated solution.

See real threats, not false positives

Over 90% of our customers have our WAF in full blocking mode. We take a threshold approach to blocking so you can run our solution in full, automated blocking mode in production with virtually no false positives. This enables you to scale protection without dealing with the maintenance overhead that legacy WAFs require.

Defeat advanced threats

Get protection that goes beyond OWASP Top 10 injection-style web attacks. We provide coverage against advanced threats including account takeover (ATO) via credential stuffing, malicious bots, API abuse and more—all in one solution.

Key benefits

- **Eliminate false positives: Over 90%** of customers are in full blocking mode
- **Trusted and proven: 90,000+** app deployments protected
- **Deploy anywhere:** From edge to on-prem with support for **100+** cloud-native and data center platforms

Fast time-to-value

Unlike traditional web application firewalls, our next-gen WAF deploys in an average of 60 minutes and you won't pay extra managed services fees for rules tuning or ongoing maintenance.

Visibility for faster remediation

Reporting and alerting feedback loops provide Layer 7 visibility across your entire app and API footprint. Integrations with DevOps and security toolchains empower teams to make decisions from the same baseline of security data provided via alerts, our API, or management console.

Betterment

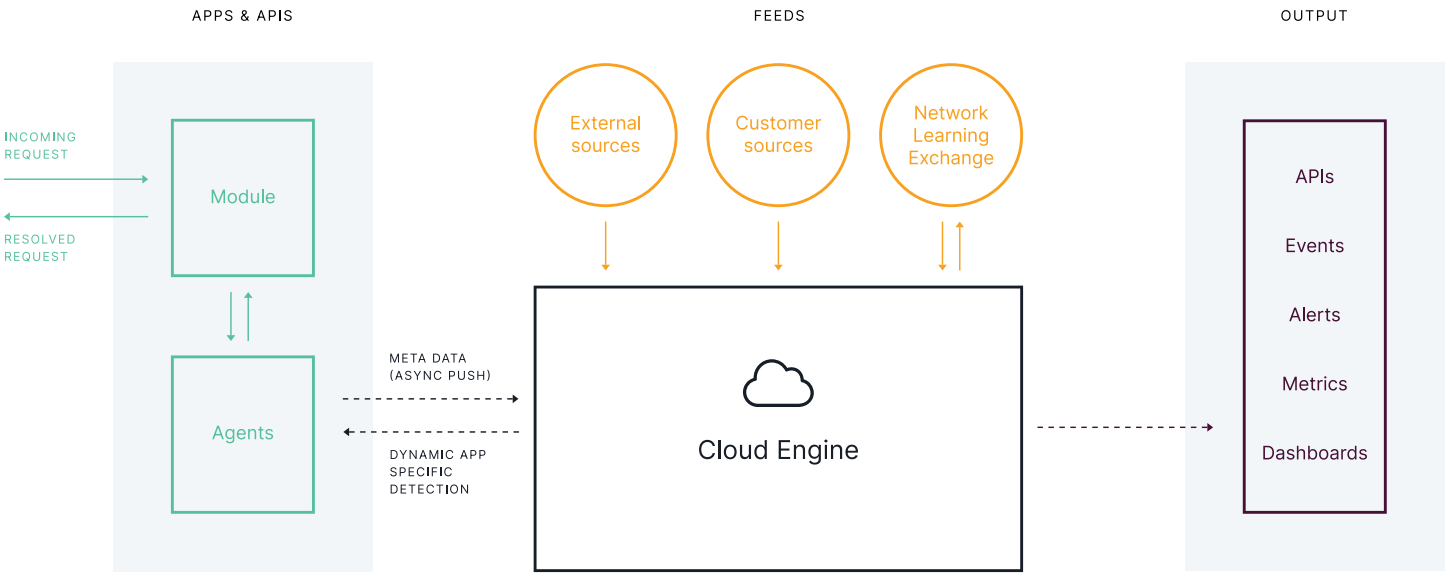
"It works straight out of the box, scales automatically, and does a great job at providing visibility while securing the application."

Anson Gomes
Lead Security Engineer, Betterment

Confidently detect and block threats

- **OWASP Top 10** - Protect against both classic OWASP Top 10 attacks and advanced web attacks.
- **Account takeover (ATO)** - Block ATO attacks by inspecting web requests and correlating anomalous activity with malicious intent.
- **API protection** - Stop API abuse by monitoring for unexpected values and parameters submitted by endpoints and blocking unauthorized requests.
- **Bot protection** - Prevent bad bots from performing malicious actions against your websites and APIs by identifying and mitigating them before they can negatively impact your bottom line or your user experience.
- **DDoS** - Prevent malicious automated traffic that aims to overwhelm or abuse your apps so they are unavailable. When defined traffic thresholds for key application functions are met we automatically block the abusive traffic.
- **Rate limiting** - Stop malicious and anomalous high-volume web requests, reduce web server and API utilization, and let legitimate traffic through to application and API endpoints with our advanced rate limiting features.

Our Patented Approach



Using lightweight software modules and agents throughout your web servers and applications, we collect information about your security posture and surface these real-time event details through self-service dashboards, intelligent alerting, and powerful reporting, powered by the Signal Sciences-developed Cloud Engine.

Unlike common regex-based WAFs, the Fastly Next-Gen WAF uses SmartParse, our highly accurate detection method that evaluates the context of each request and how it would actually execute to determine if there are malicious or anomalous payloads in requests. This feeds into our Network Learning Exchange (NLX), which recognizes attack patterns across our customer network and then proactively alerts and defends all our customers against the same attack.

Our management console quickly provides actionable information and key metrics in a centralized interface, unlike many legacy WAF vendors who require you to log in to multiple instances to gain visibility across your deployment footprint. Additionally, any request telemetry reported in our console can be ingested into your other security tools via our API.

AXON

"It's refreshing to work with a security product that not only provides exceptional security benefits, but also prioritizes performance, reliability, and overall operational manageability."

Jenner Holden
VP of Information Security, Axon

Deploy anywhere

Our deployment options provide the flexibility in development, security, and operations that teams need, enabling you to install our solution at different points in your stack, from edge to on-premises. For further detail on deployment options, see our **Architecture and Deployment Overview**.

Cloud and container-native: Our agent-module pair installs at your web server, API gateway, or at the app-level within minutes. Native integrations with container orchestration tools, like Kubernetes, and service meshes, like Envoy Proxy and Istio, provide visibility into both north-south (client-server) and east-west (service-to-service) requests.

Data center and legacy apps: The Fastly Next-Gen WAF can be installed to inspect traffic prior to web requests reaching the app or API endpoint such as at the load balancer (HAProxy, NGINX) or at the API gateway (Ambassador, Kong, Cloudentity). If your requirements don't allow for installation at the load balancer or API gateway, our agent can be deployed in reverse proxy mode.

Edge WAF: Our edge deployment bundles the best of the Fastly Next-Gen WAF, always-on DDoS mitigation inherent in our edge cloud network, and TLS management. Realize the performance benefits of our global network while simultaneously securing your traffic—all without having to deploy and manage multiple solutions.

Cloud WAF: We host the agent for you so there's no software to install. You just change your DNS record to route traffic to our hosted agent where inspection and decisioning occurs: legitimate traffic is let through to the app or API origin.

Hybrid: Have a variety of infrastructure and technology in your environment? Our range of deployment options means you don't have to cobble together different WAF solutions or leave some apps and APIs unprotected. Deploy everywhere and still get centralized management and visibility.

Remitly
Promises Delivered

"Signal Sciences [Fastly] in three words: Easy. Powerful. Magic. I would absolutely recommend Signal Sciences to other companies looking for a WAF solution that does a great job protecting environments and doesn't require a ton of time and effort to tune and manage. It gets things right the first time."

Kevin Hanaford
Senior Manager of Security & IT, Remitly

Right-sized protection

Fastly provides right-size protection to meet your business needs. Our **Secure packages** provide comprehensive web application and API protection in three easy-to-purchase options.

Feature	Essential	Professional	Premier
Fastly Next-Gen WAF, deploy anywhere	✓	✓	✓
Platform DDoS*	✓	✓	✓
TLS encryption*	✓	✓	✓
Virtual patching	✓	✓	✓
Custom signals		✓	✓
API and ATO protection rules		✓	✓
Rate limiting			✓
Eligible for Response Security Service add-on			✓
Support	By email and docs with next business day SLA	By email, docs, or support portal. 1-hour response time for urgent issues via portal	By email, docs, or support portal. 1-hour response time for urgent issues via portal.

* Customer must separately purchase a Fastly delivery product to leverage DDoS and TLS capabilities

4.9/5 Stars

Gartner Peer Insights Voice of the Customer

Signal Sciences, now part of Fastly, is the only vendor to be named a Gartner Peer Insights Customers' Choice for Web Application and API Protection (WAAP) for four consecutive years and is one of the highest-rated WAAP solutions on the market with an overall rating of **4.9/5** as of 31 January 2022[1] based on 267 reviews.

Read the report →

Getting started

Unlock highly effective security without impacting performance.

To learn more about our security solutions, visit us at fastly.com/secure or contact us at sales@fastly.com.

1: Gartner Peer Insights content consists of the opinions of individual end users based on their own experiences with the vendors listed on the platform, should not be construed as statements of fact, nor do they represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product or service depicted in this content nor makes any warranties, expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties of merchantability or fitness for a particular purpose. GARTNER PEER INSIGHTS Logo is a trademark and service mark of Gartner, Inc. and/or its affiliates and is used herein with permission. All rights reserved.