Signal Sciences
Now part of fastly

FASTLY DATASHEET

Next-Gen WAF Product Brief

DevOps and the cloud power today's software-driven world. You're shipping new apps and services across expanding infrastructure faster than ever. To protect this growing and changing footprint, you need a unified approach.

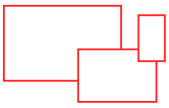
Fastly + Signal Sciences: Transforming the security landscape, together

To provide our customers with a more robust web app and API security offering, Fastly acquired Signal Sciences in late 2020. So, no matter how or where you deploy your applications, we can protect them at scale. To learn more about our leading next-gen solution, reach out to our team of security experts.

Signal Sciences
Now part of fastly

Next generation protection for your applications, APIs, and microservices

Signal Sciences protects against advanced web layer attacks and easily integrates with DevOps tools to share security data when and how your teams need it. This means you can unify the efforts of engineering, security, and operations to increase protection and maintain reliability without sacrificing velocity. With flexible deployment options, greater protection, and visibility beyond the OWASP Top 10, and more integrations into your existing tools, Signal Sciences installs easily in any infrastructure and provides fast time-to-value without rules tuning.

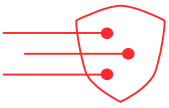


Flexible deployments

Install our software in your web server, application, PaaS, or gateway — whether on-prem or in the cloud.

Advanced attack protection

Stop OWASP Top 10 attacks, bad bots, account takeovers, DoS, and unique application abuse and misuse.



Easily integrates with DevOps tools

Access alerts and data through tools that operations and engineering teams already use.

Signal Sciences, now part of Fastly, is the only vendor to be named a Gartner Peer Insights Customers' Choice for a web application firewall (WAF) for three consecutive years, and one of the highest rated Web Application Firewall solutions on the market with an overall rating of 4.9/5 as of 31 January 2021.

Key benefits

- Over 90% of customers in full blocking mode
- 75,000+ app deployments protected
- Deploys anywhere: 100+ cloud native and data center platforms

See

Actionable, self-serve security data

Notify engineers and operations through their native tools when events occur so they can fix things fast. Our security solution is designed for agile teams making frequent changes. With intuitive dashboards and workflow integrations, all teams can self serve relevant data and security insights to understand the current security posture.

Secure

Spend less time searching, more time securing

Join the 90% of customers that block the broadest range of attack types in production: OWASP Top 10, application DoS, bots, and abuse and misuse of your application. No need to spend time looking through logs or tuning regex rules for false positives. Use the intuitive rules builder interface to define, monitor, and take action on any web application or API transaction that you create.

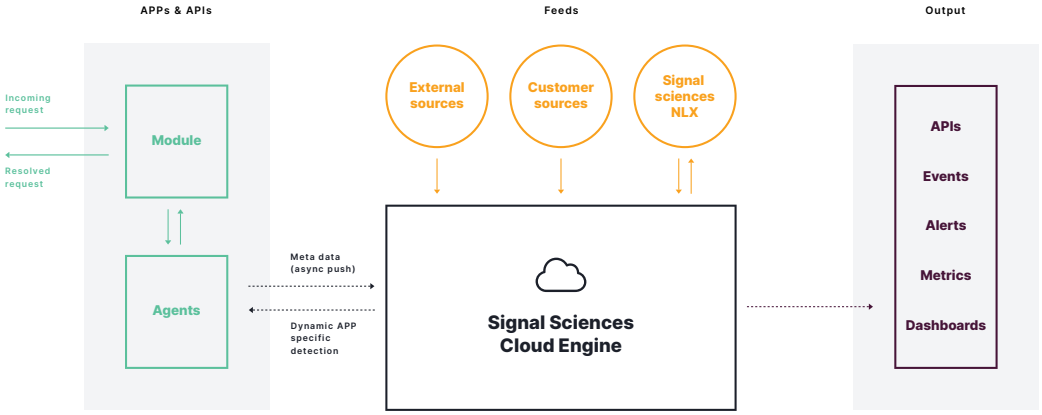
Scale

Go where no WAF or RASP has gone before

Find and fix vulnerabilities faster by monitoring your app wherever it lives — from server to code to container. Our next-gen WAF and runtime application self-protection (RASP) run anywhere with the lowest total cost of ownership, no signatures to manage, and no noticeable impact on performance.

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 Cloud Engine.



Our deployment options provide the flexibility in development, security, and operations that teams need, so they can install our web defense technology at different points in their stack. All options communicate asynchronously with the Signal Sciences Cloud Engine in the same way — with full feature parity — and deployment types can even be mixed and matched within large, complex applications managed by different teams.

A single management console provides actionable information and key metrics quickly in a single centralized interface, unlike many legacy WAF vendors who require you to log in to multiple tools to gain visibility.

More than a WAF

	Legacy WAFs	Signal Sciences next-gen WAF
Deployment mode	91% run in log or monitor mode only, or shut their WAF off completely due to false positives[1]	Over 90% of customers in full blocking mode
Architecture compatibility	Physical or virtual appliance: Poor for use with cloud CDN: No unified management across different CDN WAF products	Same architecture and UI for unified management across all app deployments: web servers; app servers; PaaS; native, hybrid and multi-cloud; on-prem; serverless; containers
Attack types	OWASP Top 10 only	OWASP Top 10, DoS, brute force/ ATO attacks, app abuse and misuse, bad bots
Enables DevOps	Rarely used or accessed outside security, poor toolchain integrations	Full alert details available to DevOps and security via Slack, Jira, Pagerduty, Splunk, and dozens more

[1] *Reaching the Tipping Point of Web Application and API Security, ESG Research, July 2021*

About Signal Sciences, now part of Fastly

We make web applications more secure. Simple as that. We provide web protection that security, operations, and engineering teams actually want to use. Learn more at fastly.com.