Product Brief

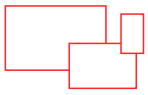
Summary

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 front.

Next generation protection for your applications, APIs, and microservices

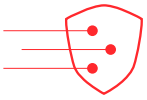
Signal Sciences protects any app, against any attack, and integrates with any DevOps toolchain. It is designed to unify the efforts of engineering, security, and operations to increase protection and maintain reliability without sacrificing velocity.

With flexible deployment options, greater protection, and visibility beyond 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.



Any App

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



Any Attack

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

Any DevOps Toolchain

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

Gartner peerinsights customers' choice™

★★★★★

2019 | 2020 | 2021

Fastly (Signal Sciences) named a Gartner Peer Insights Customers' Choice for WAF for three consecutive years and the only major WAF with a 5 out of 5 overall rating.

Key Benefits

- **95% of Signal Sciences customers** are in full blocking mode in production
- **Four out of five** who try us, choose us to secure their web apps, APIs, and microservices
- **Deploys under an hour** on average
- **Protects apps in any infrastructure** including cloud, on-premise, or hybrid environments

SEE

Actionable, self-serve security data

Notify engineers and operations through their native tools when events occur so they can fix things fast. Signal Sciences 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 95% of customers who block across the broadest 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 Power Rules interface to define, monitor, and take action on any web application or API transaction that you create.

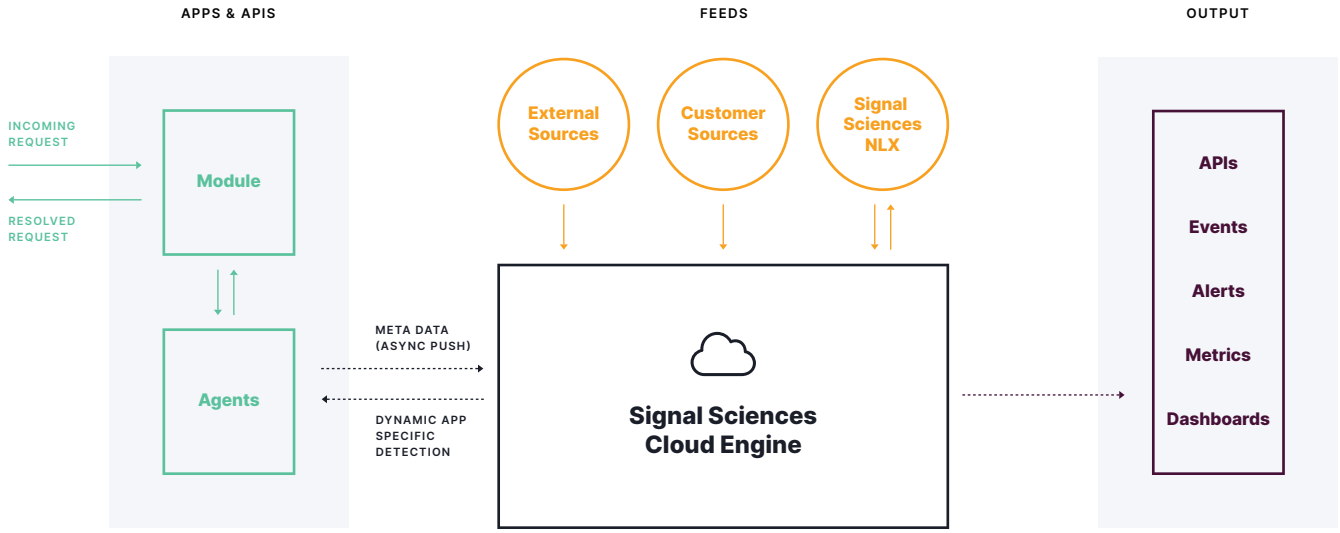
SCALE

Go where no RASP or WAF 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 RASP run anywhere with the lowest total cost of ownership, no signatures to manage, and no noticeable impact on performance.

Our Patented Approach

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



Our deployment options provide the flexibility development, security, and operations 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 legacy WAF vendors who force you to login into multiple tools to gain visibility.

> **“ The Signal Sciences approach gives us situational awareness about where and how our applications are attacked so that we can best protect ourselves and our customers.**

Jon Oberheide, Co-Founder & CTO, Duo

More than a WAF

	Legacy WAFs	Signal Sciences Next-Gen WAF
Blocking Mode Enabled	– Estimated at <10% based on customer feedback	✓ 95% in blocking mode for all attacks
Architecture Compatibility	– Physical or Virtual appliance (e.g. F5, Imperva): *Poor for use with cloud* CDN (e.g. Incapsula, Akamai Kona): *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, Application abuse and misuse, Bad bots
Deployment Time	– Months	✓ Average is 60 minutes (record is under 1 minute)
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
Virtual Patching	✓	✓
PCI 6.6 Compliance	✓	✓

The world's top companies trust Signal Sciences

one medical · CHEF · THRIVE MARKET · DATADOG · Betterment · DUO · SHINOLA DETROIT · UNDER ARMOUR · onelogin · asurion · snapdocs