Signal Sciences

Signal Sciences Next-Gen WAF

BENEFITS

- Reliable, automated blocking of attacks
- DevOps focused protection
- Platform agnostic with unified management
- Coverage across all threats

Your application footprint is growing more complex and varied with faster development cycles and the shift to cloud, whether hybrid or public. These applications are providing new and engaging experiences for your customers, which means more data to protect. Having a single pane of glass for web defense across your mix and match application environments is critical to driving your business forward, and security can't be a blocker. Legacy rules-based web application firewalls (WAFs) won't scale, and a next-gen approach is needed.

At Signal Sciences, we believe security has to become tightly integrated with all teams. Our easy to install software supports any application without impacting performance to protect against any attack, with integrations to any DevOps toolchain products for cross-team visibility.

Why Companies Choose Signal Sciences

Reliable, automated blocking of attacks

- Our lightweight modules run directly in your web servers or application code using a patented, fail-open architecture to communicate with a local agent, which means your site stays up and running fast.
- Our token-based approach to attack detection is more accurate than rules or signatures and requires no tuning or maintenance.
- Agents collect and send detection data asynchronously to our proprietary cloud decision engine to look at data across your applications to send down decisions with details explaining why a block was made.

> More than 95% of customers deploy Signal Sciences in blocking mode in production.

Legacy web application firewalls (WAF) have been traditionally deployed at the edge, making it impossible to see what's getting through to the origin or application behavior. They are also a single point of failure to your application and can add latency to the request, impacting the user's experience. Rules are costly to write and maintain, and when triggered, don't show request details so few ever make it to blocking mode.

DevOps focused protection

- Operations can easily deploy and scale our software with metrics on how it's performing, typically with fewer than 3 milliseconds of latency.
- Pushing security data to tools used by developers, operations, and security teams allows teams to work together to self-service data and fix issues faster.
- Robust APIs allow SOC teams to pull data into SIEM tools to visualize trends over time and better prioritize resources.

WAFs become difficult to manage as instances are difficult to stand up as applications and services scale. Integration capabilities with DevOps tools are not widely supported, limiting visibility for teams to access security data. APIs, if available, are hard to parse and consume.

Platform agnostic with unified management

- Signal Sciences provides the most flexibility to deploy anywhere in your technology stack, whether in containers, on-prem or in the cloud.
- Central management and unified views across your entire footprint provide unparalleled reporting to the entire organization.
- Internal sites and services can be protected and monitored even if they're not exposed to the public Internet.

WAFs can be limited by the CDN technologies they're connected to; different CDN choices require management of separate WAF products. CDN WAFs can't be used to detect attacks on internal applications since they're deployed at the edge.

Coverage across all threats

- Gain immediate blocking from common OWASP attacks without tuning a single rule.
- Go beyond OWASP to block account takeovers (ATOs), bad bots, application denial of service (DoS), and apply virtual patches against known CVEs.
- Meet your PCI 6.6 compliance requirements in addition to our automated blocking benefits.

Other WAF approaches don't have the same flexibility to monitor and protect against application abuse and misuse. Custom rules can require days, weeks, or even months in turnaround time to propagate to your sites.

Any App

Cloud, Containers, PaaS, and Serverless

Web Servers and Languages

Gateways and Proxies

Any Attack

OWASP Top 10

Application DoS

Brute force attacks

+ MORE

Any DevOps Toolchain

Slack

HipChat

Datadog

Webhooks

Splunk

SIEM/SOC tools via APIs

+ MORE