Signal Sciences

Signal Sciences RASP

BENEFITS

- DevOps focused protection
- Platform-agnostic with unified management
- Reliable, automated blocking of attacks
- 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. Runtime application self-protection (RASP) has emerged as an alternate way to secure apps, but they're not all built the same.

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

DevOps focused protection

- 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.
- Integrations to DevOps tools with event details allow engineering, operations, and security teams to work together and fix issues faster.
- Robust APIs allow SOC teams to pull data into SIEM tools to visualize trends over time and better prioritize resources.

Other RASP products interrupt the DevOps workflow, starting with a heavyweight installation process that requires black-box library inclusions or JVM replacements that are hard to install, troubleshoot, and scale. Without detection and decision details, any available APIs and other integrations lack information to help teams diagnose root cause. With all application logic in the agent versus our module-agent design, these other RASP approaches fail closed, causing latency and app failure if run in blocking mode.

Platform-agnostic with unified management

- Lowest total cost of ownership comes with the ability to use one tool to provide comprehensive protection.
- 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 application footprint provide unparalleled reporting to the entire organization.

Other RASP approaches can't provide full coverage due to limited language support. You're left with partial coverage of your application footprint or forced to use another tool that comes with added overhead to operationalize. Unique instrumentation is required per application language to gain basic OWASP vulnerability coverage. This leads to long rollout times due to tuning and instrumentation processes.

Reliable, automated blocking of attacks

- Without learning or tuning, Signal Sciences provides immediate visibility and the ability to block attacks right after installation.
- Our token-based approach to attack detection is more accurate than rules or signatures and requires no tuning or ongoing 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.

Other RASP products are rarely used in blocking mode because most are prone to high false positives due to the use of regular expression rules deployed in your application code. They show little to no information around what causes application errors, making troubleshooting difficult. Some even require a "learning mode" to determine rules, leaving the application unprotected when you make changes to your application.

Coverage across all threats

- Gain immediate blocking from common OWASP attacks without tuning a single rule.
- Use our simple UI to go beyond OWASP and 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 RASP products don't have the same flexibility to monitor and protect against application abuse and misuse, since their logic is hard coded into their agents. Account takeover (ATO) protection is only provided by select vendors, and beyond ATO, there is no user interface or ability to customize policies beyond ATO.

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