Signal Sciences

Protect your most critical web apps, APIs, and microservices.

Signal Sciences is the industry's first Web Protection Platform that works in any cloud, container, PaaS, and any modern application architecture — allowing you to securely embrace the shift to Agile, DevOps, and the Cloud. The Signal Sciences Web Protection Platform can be deployed in Next Generation Web Application Firewall (NGWAF), Runtime Application Self Protection (RASP), or Reverse Proxy modes giving your company the ultimate flexibility and coverage.

Adobe · Under Armour · Shinola Detroit · one medical

Etsy · Duo · wework · Betterment

tenable · SendGrid · greenhouse · vimeo

"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 SECURITY

Duo

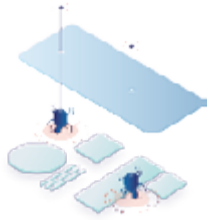
Signal Sciences

How Our Process Works

1. When an incoming HTTP request is received by your web server, the module forwards the request to the agent via a local unix domain socket or the loopback interface.

2. The agent analyzes the request, typically in less than a couple of milliseconds, and responds to the module with a decision to block or allow the request. To provide a hard guarantee on performance and reliability, if the agent doesn't respond within a configurable timeframe, the module will allow the request through to the application.

3. After identifying any malicious signals in the request, the agent sends only the relevant malicious portions to the Signal Sciences cloud decision engine for further analysis. For performance and privacy reasons this step is performed asynchronously and only request metadata is sent to the cloud backend.

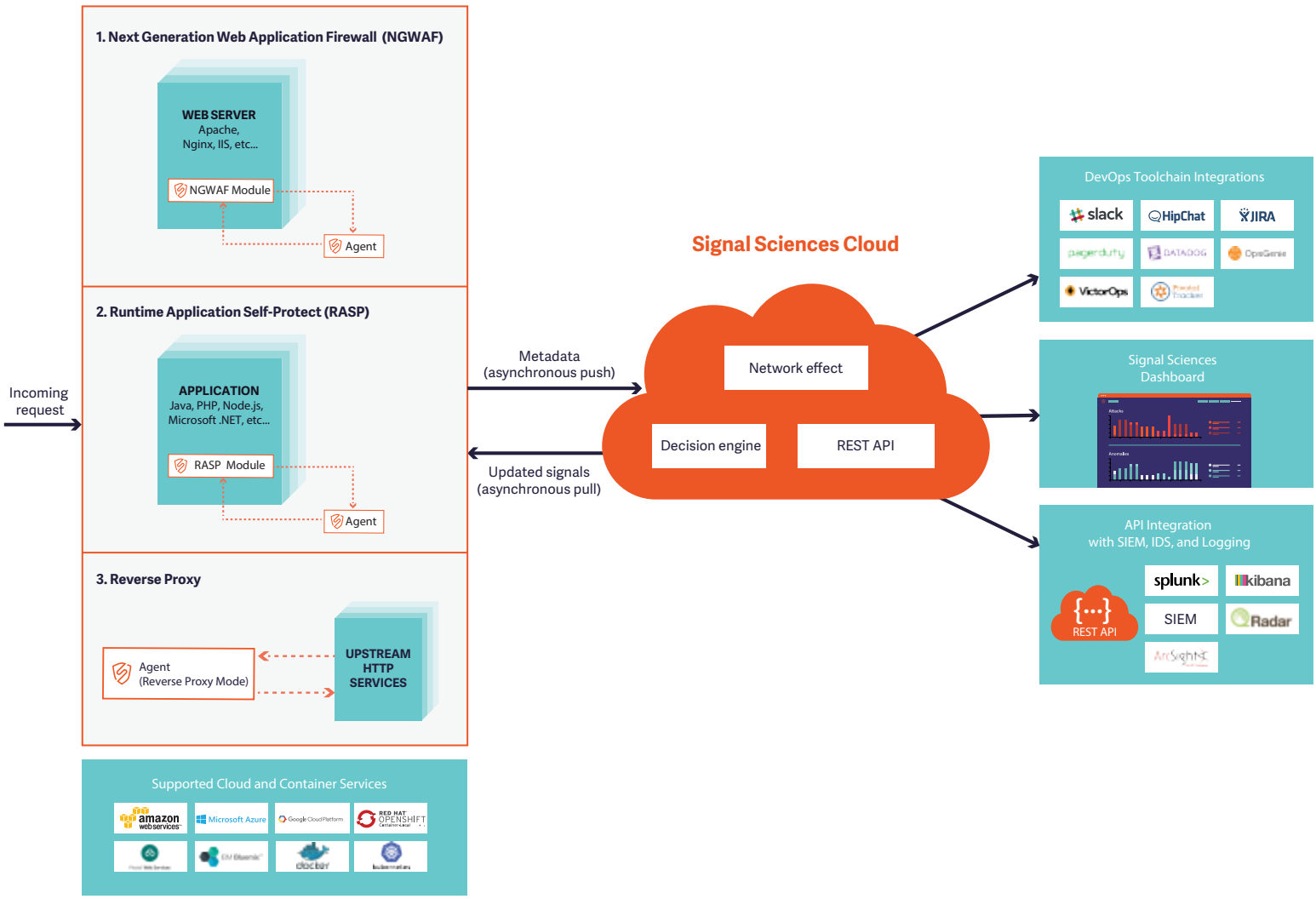


4. When an attack is identified, the Signal Sciences cloud decision engine will generate an updated blocking rule that is received and cached locally by the agent. Subsequent malicious requests from that source are then automatically blocked while still allowing legitimate traffic through.

5. Visibility is provided via dashboards and one-click integrations are available for a number of common third party services. The API-First implementation of the dashboards means all data can be easily fed into existing central logging and SIEM systems.

Signal Sciences

Deployment Options



"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. Signal Sciences is easy for our devops team to support, which allows us to focus on the security capabilities it provides, rather than fighting with basic operational issues."

Jenner Holden

VP OF INFORMATION SECURITY, AXON (PREVIOUSLY TASER INTL.)

AXON

Signal Sciences

Signal Sciences Web Protection Platform

The only solution built by practitioners who have faced the same challenges that our clients see:

Securely embrace DevOps.

With more than 15 integrations, Signal Sciences embraces how your security, operations, and development teams do business by integrating into their most common tools, including Slack, Jira, Hipchat, PagerDuty, Datadog, Splunk, and more.

Any cloud, any infrastructure, any technology.

By offering a menu of different deployment choices (NGWAF, RASP, and Reverse Proxy modes), we can support all of your applications -- regardless of infrastructure, language, containers, or cloud deployment choices.

Defensive coverage without breaking the app. Seriously.

Over 95% of customers use Signal Sciences in full blocking mode in production, with no learning, tuning, or false positives. Signal Sciences WPP goes beyond the OWASP Top 10 attacks. The WPP protects you from common attacks, such as SQL injection and cross-site scripting, as well as more modern threats, such as application DDoS, brute force attacks, and attacks against your applications' sensitive business logic.

Flexible deployment options:

Next generation web application firewall
Runtime application self-protect (RASP)
Reverse proxy

Signal Sciences host-based deployment model means:

No application code changes
No hardware/VMs to deploy

With Signal Sciences, our clients are able to:

Use any CDN.

Akamai, CloudFront, Edgecast, etc.

Use any physical infrastructure, cloud provider, or PaaS.

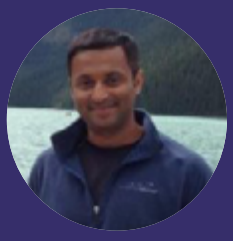
AWS, Google, Azure, Heroku, Pivotal, IBM Bluemix, etc.

Use any container.

Docker, Kubernetes, Red Hat OpenShift Container, etc.

Use any configuration management.

Chef, Puppet, Ansible, etc.



"Signal Sciences has given us confidence in our application security posture especially for current and future acquisitions. Their architecture and install process make it seamless to start recieving real-time attack telemetry so that we can prioritize our defensive efforts based on actual attacks."

Vivek Ramen
SECURITY MANAGER AT YELP

yelp EAT24

122 MILDRED AVE
VENICE, CA 90291

INFO@SIGNALSCIENCES.COM
SIGNALSCIENCES.COM