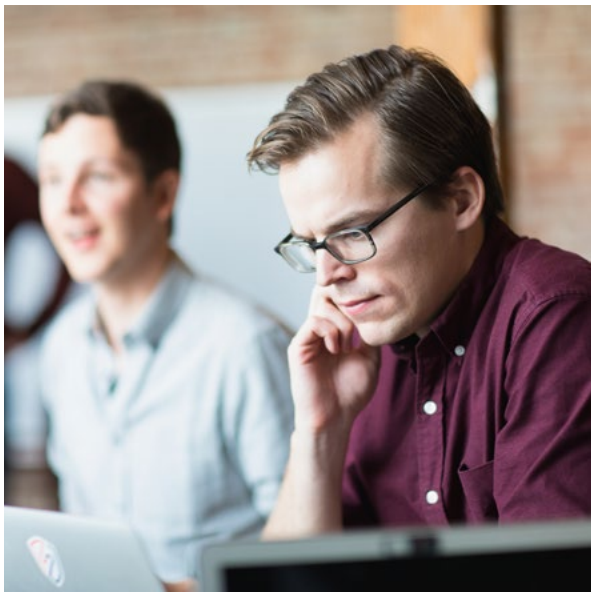
Signal Sciences Web Protection Platform: Next Generation Web Application Firewall



> Signal Sciences Web Protection Platform includes a Next Generation Web Application Firewall (NGWAF) which provides advanced defense for web applications.

The NGWAF installs as a lightweight module with all popular web servers and is entirely software based so it can fit in cloud architectures and containers or in your own datacenter. Installation is simple, allowing you to secure your applications, APIs and microservices in minutes.

Why Companies Are Choosing Signal Sciences NGWAF Solution

It's fast. Signal Sciences NGWAF was built for high performance and scalability, and unlike traditional WAFs that added hundreds of milliseconds of latency, our NGWAF adds 2-3 milliseconds of latency. You won't even know it's there.

Works with all popular web servers. Whether you are using NGINX, IIS, Apache or Tomcat, we have you covered. Our NGWAF is able to plugin via a module built for your particular web server.

Advanced detection over signature based approaches. Signal Sciences advanced detection is a proprietary technique that analyzes request parameters and tokenizes the results. The tokenized representation of the request is analyzed, at runtime, to detect attacks and is much faster and more accurate than regex and signature-based approaches.

Protect against the OWASP Top Ten and more. Using Signal Sciences NGWAF, you are protected against XSS, SQLi, command execution and the rest of the OWASP Top Ten. The OWASP Top Ten is just the beginning. We also protect you from application denial of service, malicious bots, account takeover, and can even help secure your unique business logic.

Application insight without any code changes. With Signal Sciences NGWAF you are able to get insight into attacks against your application. Out of the box you get protection against common application attacks, however you additionally gain the ability to easily instrument any area of your application. This means real time insight into sensitive business logic and authentication without any code changes to the application.

Virtually zero false positives. Working with traditional WAFs is a constant battle in fighting false positives. Signal Sciences works by scoring traffic and only taking defensive measures when there is divergence from normal traffic thresholds. This means you can run in production without breaking your application.

Over 95% of Signal Sciences customers are in full blocking mode for their production traffic. You can gain defensive coverage of your entire application landscape without breaking production systems.

No bottlenecks or single points of failure architecture. As hands-on operators ourselves, we didn't want to add any bottlenecks or single points of failure to our system and certainly not to our customers. Our design and architecture is build around an asynchronous model that means your uptime and availability won't be negatively impacted by Signal Sciences.

Meets compliance and provides real protection. Signal Sciences NGWAF fulfills the role of the traditional WAF for compliance purposes but adds insight and protection that wasn't previously available.

Scales as you grow. You are free to scale up to hundreds or thousands of containers or cloud instances and then back down without any additional licensing. We work with you to protect your applications and your licensing model isn't based on CPUs or number of servers or instances.

Signal Sciences NGWAF Technical Specifications

Web servers supported

- NGINX
- Apache
- IIS
- Tomcat
- Node.js Express

Integrates directly into your DevOps toolchain

- Slack
- HipChat
- Generic Webhooks
- DataDog
- OpsGenie
- VictorOps
- PagerDuty
- Full API access

Integrates into your SIEM/SOC

- Splunk
- Elastic/ELK
- Arcsight
- QRadar
- Any custom tools via a full REST JSON API

Covers all modern attack types

- OWASP Top 10
- Application DDoS
- Brute force attacks
- Sensitive business logic attacks
- Request rate limiting
- Account takeover attacks
- Bad bots and scrapers