

# Cloud WAF

*Signal Sciences Cloud WAF makes it easy to protect the web layer assets that drive your business without dedicating headcount or additional resources*

## SUMMARY

Signal Sciences Cloud WAF protects your web layer assets quickly with just a single DNS change. There's no "learning mode" period and rules maintenance overhead that rules-based legacy WAFs require.

## The Challenge

Organizations know that the success of protecting their applications wherever they operate—cloud, on-premise, or hybrid environments—depends on their ability to prioritize headcount, budget, and time. But they must balance those needs against continuous deployment while securing the applications, APIs and microservices that drive their business. Security and development teams expected to safeguard digital assets at the web layer often lack in-house expertise to install and manage a WAF or other application security tools. They need a web application security solution that:

- Deploys quickly and easily
- Requires no additional headcount
- Seamlessly protects both cloud and legacy applications
- Provides actionable insights and alerts to create feedback loops

## Cloud WAF: Easy Deployment for Web Protection that Scales

With a single change to a DNS record, web requests are routed to the Signal Sciences Cloud Engine to inspect and decision on those requests and block bad requests. Our unique solution provides robust detection and protection capabilities no matter where your organization's applications reside: cloud, on-premise, hybrid or containers. Cloud WAF operates without complex software installation or agents, even as application growth scales.

Leveraging the same patented next-gen WAF technology as our other deployment options, Cloud WAF provides advanced protection capabilities including Power Rules and Network Learning Exchange (NLX) that provide precise instrumentation and request context that stops any attack against any app deployed in any infrastructure. With a single management console, security and development teams get clear actionable insights without digging through several different interfaces. Integrations with DevOps tools like Slack, PagerDuty and Jira provide real-time alerting your team needs to stay ahead of the adversary.

## KEY BENEFITS

- No agents to deploy
- Scales quickly to protect new and legacy applications
- Protects your apps wherever you deploy them: cloud, on-premise or hybrid environments
- Fast time to value for security, DevOps and operations teams

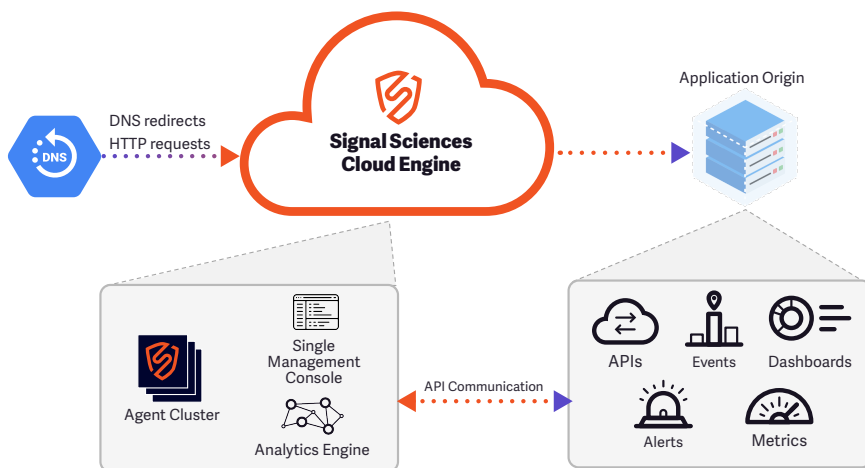
## Secure Serverless with Cloud WAF

Serverless enables companies to build applications with increased agility and lower total cost of ownership while shifting infrastructure management to the cloud provider. This new serverless model focuses on distributed apps, APIs, and microservices in stateless containers. Signal Sciences Cloud WAF enables developers designing and deploying in cloud infrastructure to monitor East-West web request traffic between microservices, ensuring that malicious requests are detected and stopped no matter their origin.

### How Cloud WAF Works

Signal Sciences deploys an agent in reverse proxy into the Signal Sciences Cloud Engine. When the customer performs the CNAME DNS record change, all inbound web requests are redirected to Signal Sciences agents functioning in a reverse proxy mode to the customer's origin web server on a publicly accessible IP address. Signal Sciences manages and deploys agents as close as possible to customers' application origin servers to:

- Minimize latency
- Scale protection across additional cloud infrastructure, as necessary
- Manage and maintain any additional agent deployment



*Cloud WAF operates without complex software installation even as application growth scales. With a DNS change, all web requests are redirected to the Signal Sciences Cloud Engine where bad requests are detected and blocked. All good, legitimate traffic is forwarded to the customer's application origin server.*

#### KEY PRODUCT CAPABILITIES

- **No agents to deploy and manage:** superior web app layer protection with just a DNS change
- **Effective protection:** 95% of customers use Signal Sciences in full blocking mode in production
- **Deploys in minutes, not days or months:** deploys on average under an hour
- **Protect your applications no matter where you host them:** cloud, containers, on-premise or hybrid environments
- **Full feature parity:** provides the same detection and protection capabilities of other Signal Sciences deployment methods with the same actionable insights, reporting and DevOps tool integrations.
- **Single management console:** get 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.