Architecture Overview

Signal Sciences is the only two-time Customers' Choice for WAF and the only major WAF with a perfect 5 out of 5 overall rating.

Signal Sciences Web Application and API Protection Platform provides the proactive protection modern apps require while integrating into any DevOps toolchain for unparalleled visibility. Our flexible architecture can advance your application security strategy by providing developers, operations, and security teams insight into where and how your web applications and APIs are attacked.

Gain comprehensive protection without sacrificing performance, with no training or dedicated employees required: Signal Sciences simply works out of the box to detect and stop malicious traffic directed at your apps and APIs.

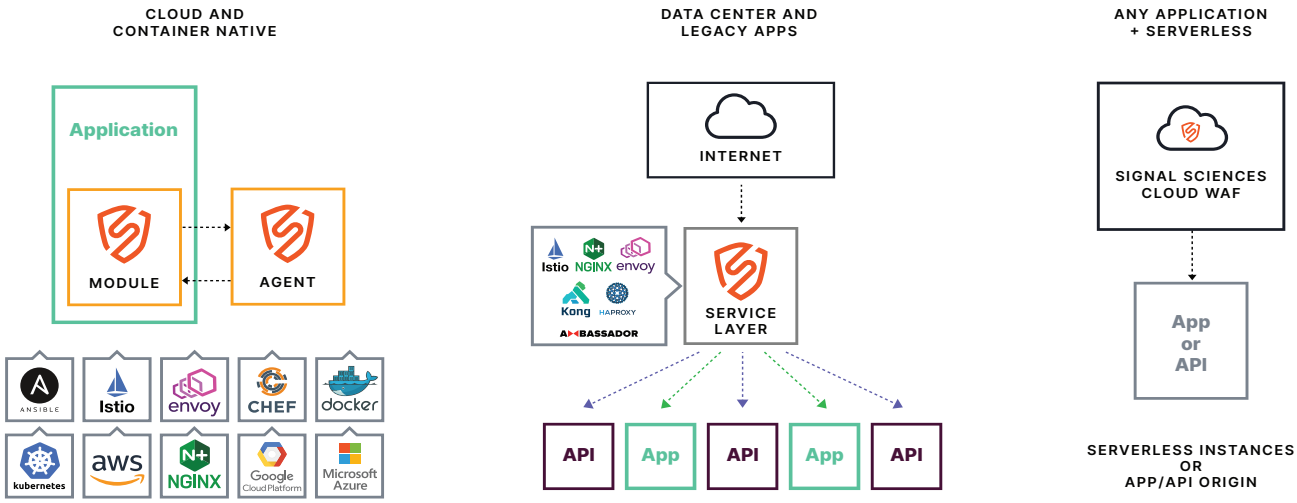
This Architecture Overview provides technical insight into how and why the world's leading companies use Signal Sciences Web Application and API Protection Platform to secure their web applications, APIs, and microservices at scale. This document is arranged into three key sections:

- **Architecture Overview and Deployment Options**
- **Key Benefits and Differentiators**
- **DevOps, SOC, and SIEM Toolchain Integrations**

Deployment Overview and Options

Native Deployment Options For Datacenter, Cloud, Containers, and Serverless

Signal Sciences provides a hybrid SaaS solution that can be deployed in the cloud, in front of legacy applications, or with a single DNS change and no agents.



Protection that won't impact app performance

We deliberately designed and patented our agent and module components to work together reliably to protect your apps and APIs without impacting their performance. This is why the highest scale applications and APIs on the Internet use Signal Sciences to provide protection without sacrificing performance or reliability.

Legacy WAFs and other RASP implementations store all of the logic in one component, which can cause app crashes or errors when the software misbehaves or is under high load: if they go down, traffic to your app is blocked, negatively impacting your business.

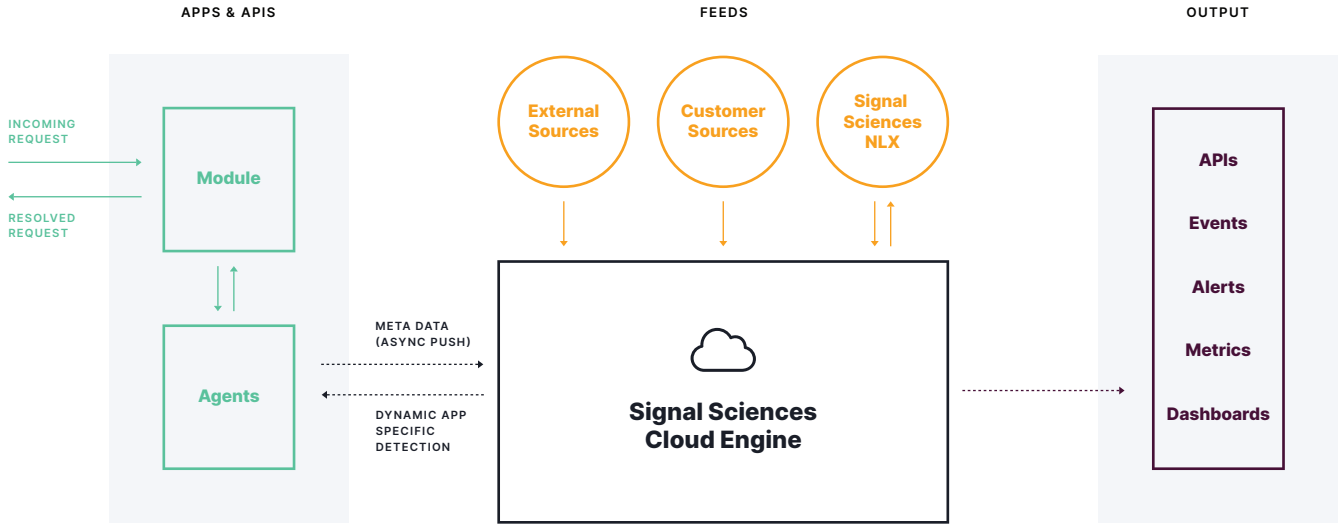
Protection that's committed to data privacy

The world's leading financial services firms, healthcare companies, and others with strict data privacy requirements all utilize Signal Sciences because of the strong architectural guarantees built for data privacy. All sensitive data is handled entirely within the customer environment and never sent to the Signal Sciences cloud backend. After our agent pre-filters locally to determine if the request contains an attack, only sanitized and redacted portions of requests that are marked as attacks or anomalies are then sent to the Signal Sciences backend.

Once the agent identifies a potential attack or anomaly in a request, a set of fully customizable redactions are applied locally and then the agent sends only the redacted individual parameter of the request which contains the attack payload, as well as a few other non-sensitive or benign portions of the request, such as client IP, user agent, URI, etc. Our backend only collects the response's metadata e.g. response codes, sizes, and times.

For additional protection, Signal Sciences automatically enforces redaction of common sensitive data types - such as passwords, keys, GUIDs, and any type of PII or PHI - before the request is sent to our backend. We also provide customers the ability to fully customize redaction policies and fields as needed.

Deployment Option 1: Cloud Native



Signal Sciences is a hybrid software as a service (SaaS) solution with two main components:

1. **Signal Sciences Agents and Modules:** Server-side software you install on your infrastructure within minutes, via public repositories and configuration management tools
    - **Signal Sciences agents**: small agents that you deploy on your existing infrastructure perform detection and decisions against requests quickly and accurately
    - **Signal Sciences modules**: an optional but powerful component that pairs with the agents to enforce high performance and reliability guarantees

2. **Signal Sciences Cloud Engine:** our cloud-hosted analytics backend enriches the agent asynchronously with intelligence gathered from external and proprietary sources to make dynamic, application-specific detections

In addition to the web server integration module and monitoring agent, our cloud-hosted backend analyzes the harvested telemetry. When traffic reaches the server, the module passes the request to the agent which then determines if the request is malicious. The agent responds back to the module to block or log the traffic based on the mode. All detection takes place at the agent level within your infrastructure. The agent collects metadata about the malicious requests it has processed and shares that metadata with the Cloud Engine.

Modules

Modules run on virtually any web server (NGINX, Apache, IIS, and more) or application language (.NET, Java, Python, PHP, .nodeJS, and more). The module is just a few hundred lines of code to ensure both reliability and

extreme performance. Its sole job is to pass requests through to the agent and receive and enforce decisions from the agent to allow the request through to the application or log/block it (depending on the mode set in the Console).

Agents

Signal Sciences agents are designed to handle extremely heavy loads while making highly-performant and accurate detections and decisions locally. We protect some of the highest volume sites on the Internet, where tens of thousands of agents collectively process trillions of production requests without impacting app or API performance. Agents block attacks before they hit applications or APIs and provide visibility into not only requests that come in, but also server responses and anomalies that show how the application is behaving.

Cloud Engine

The Cloud Engine collects anonymized attack data that the many thousands of software agents collect from across our customer base. The output from the Cloud Engine is used by the agent locally to perform better detection and make more aggressive blocking decisions. The agent decisioning is enhanced by NLX—or Network Learning Exchange—that shares confirmed malicious IP sources within Signal Sciences management console, alerting you to suspicious actors before they are a threat to your applications and APIs. Other feeds include external lists of malicious IPs, customers' custom IP lists, and NLX, all of which provide additional request context that enriches the agent decisioning. This visibility and context is shared via our API and native integrations with the DevOps tools your team already uses, including Slack, PagerDuty, Jira and more. Metrics and event reporting for your entire application footprint is also readily available via dashboards in a unified management console.

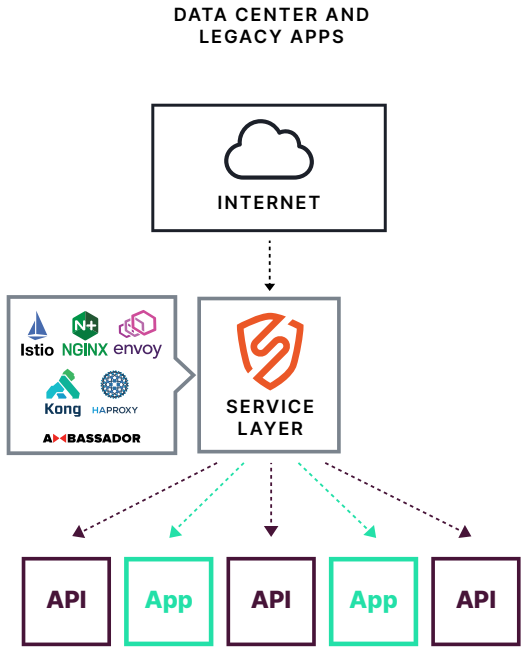
Deploying in Kubernetes and Service Mesh

New application tools and frameworks, such as Kubernetes, are quickly moving companies into a DevOps-focused world. Companies now release code faster than ever before and Signal Sciences offers flexible deployment options to fit within your container strategy with three "layers" where you can install Signal Sciences in Kubernetes, and four methods for how you deploy. Additionally, our native integrations with Envoy Proxy and Istio service meshes mean Signal Sciences provides visibility into both north-south (client-server) and east-west (service to service) requests.

Install Method	Layer 1: Ingress Controller	Layer 2: Mid-Tier Service	Layer 3: App Tier
Agent + module in same app container	✓	✓	✓
Agent + module in different containers	✓	✓	✓
Agent in reverse proxy mode in same container as app	✓	✓	✓
Agent in reverse proxy in sidecar container	✓	✓	✓

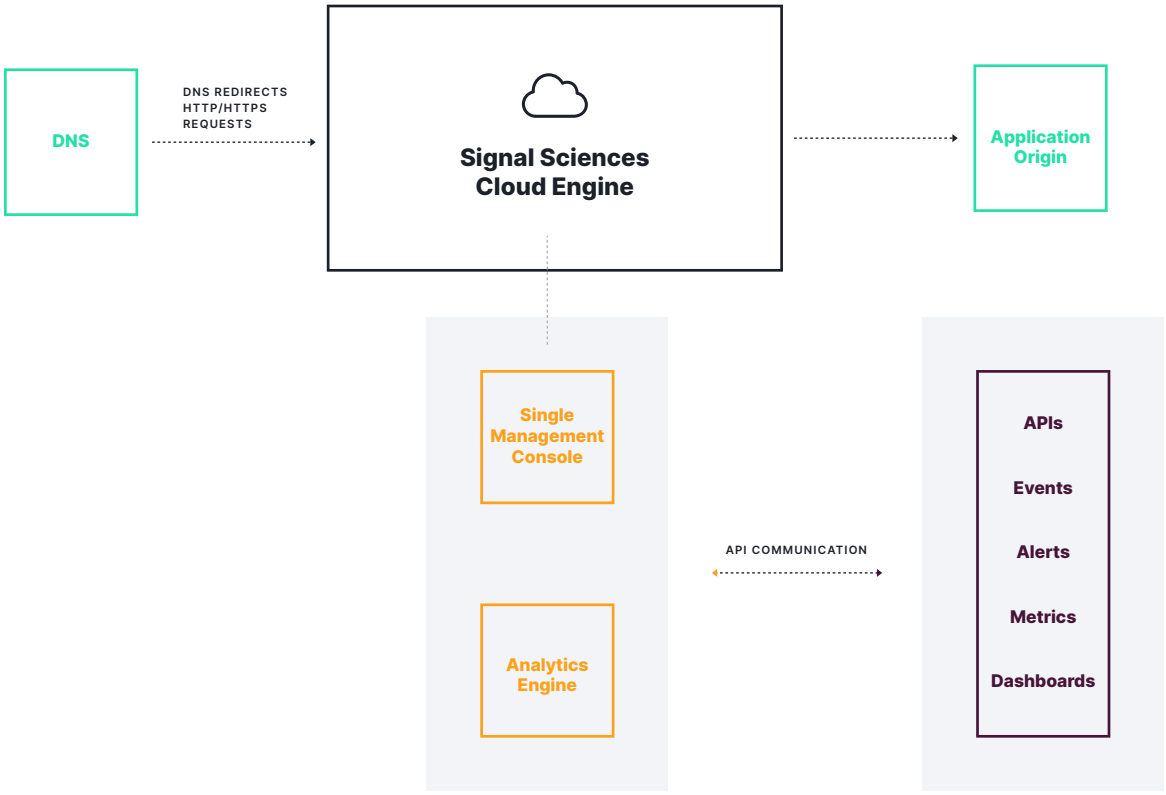
Signal Sciences fully supports deployments for: kubernetes docker envoy Istio

Deployment Option #2: Data Center and Legacy Applications



Customers who need protection for legacy applications or those deployed in data centers typically choose one of two deployment options: install Signal Sciences to inspect traffic prior to web requests reaching the app or API endpoint or install our agent in reverse proxy mode. For example, our module can be installed at the load balancer (HAProxy, NGINX) or at the API gateway (Ambassador, Kong, Cloudentity). For customers with requirements that don't allow for installation at the load balancer or API gateway, our agent can be deployed in reverse proxy mode. Either deployment option provides the same level of visibility and actionable insights and alerts as our other deployment options with full feature parity.

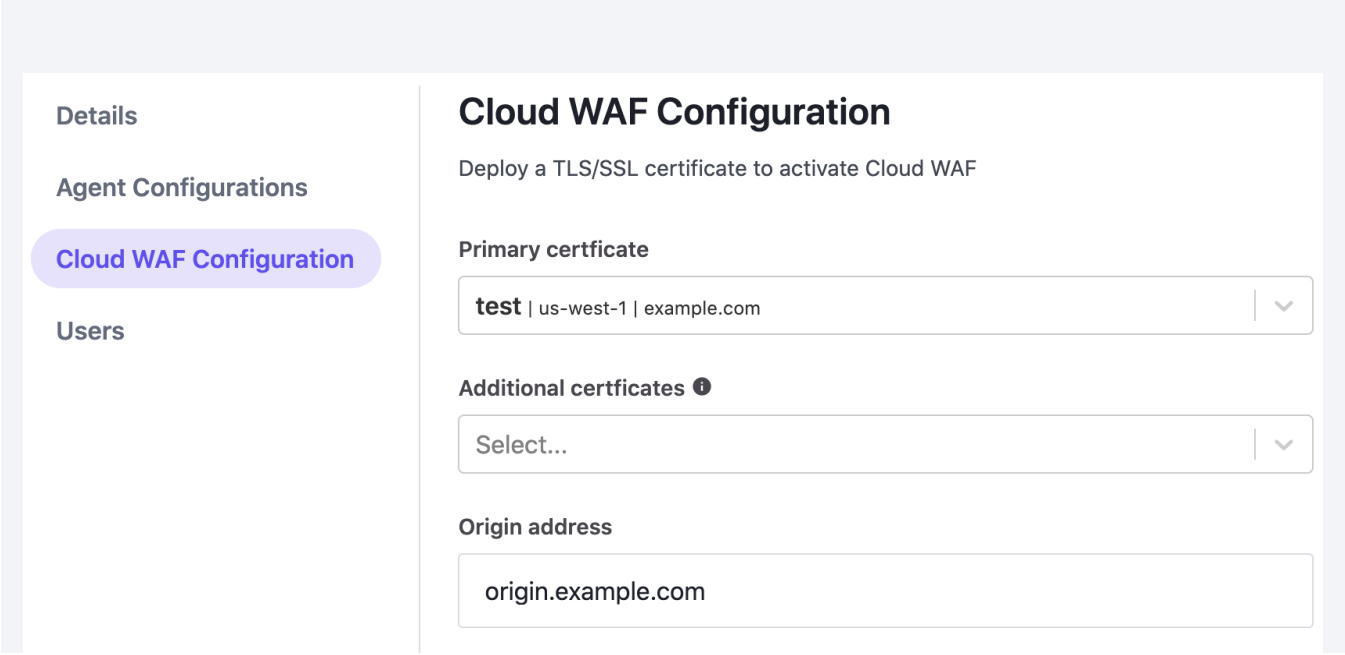
Deployment Option #3: Any Application + Serverless



Our Cloud WAF deployment option protects serverless instances and other applications where installing the agent-module pair is not an option.

Signal Sciences Cloud WAF empowers organizations to quickly and easily protect web applications, APIs and microservices—without dedicating headcount or additional resources. 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 then forwarded to the customer's application origin server.

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 serverless architecture to monitor web request traffic and protect their serverless applications, ensuring that malicious requests are detected and stopped no matter their origin.



Cloud WAF can be deployed in a matter of minutes, requiring only an uploaded TLS certificate and a few basic parameters such as origin address.

Once deployed, a simple DNS change to point application traffic to Cloud WAF is all that's needed to enable the visibility and protection of the Signal Sciences Platform for your applications.

Key Benefits and Differentiators

We provide customers application and API protection by inspecting web requests and detecting and blocking malicious and anomalous web traffic directed at your applications, APIs and microservices wherever they run. The flexibility and efficacy of our protection can be summarized in the following benefits:

False Positives

95% of Signal Sciences customers utilize full blocking mode within hours/days, rather than being stuck in monitor or "learning" mode due to false positives.

Coverage

Far beyond OWASP Top Ten, Signal Sciences provides coverage over Malicious bots, Account Takeover/Credential Stuffing, API Abuse, App DDoS, Advanced Rate Limiting, Virtual Patching and more.

Performance

Signal Sciences patented performance guaranteeing architecture protects trillions of web requests per month for the most performance-sensitive global enterprises on the planet.

Deploy Time

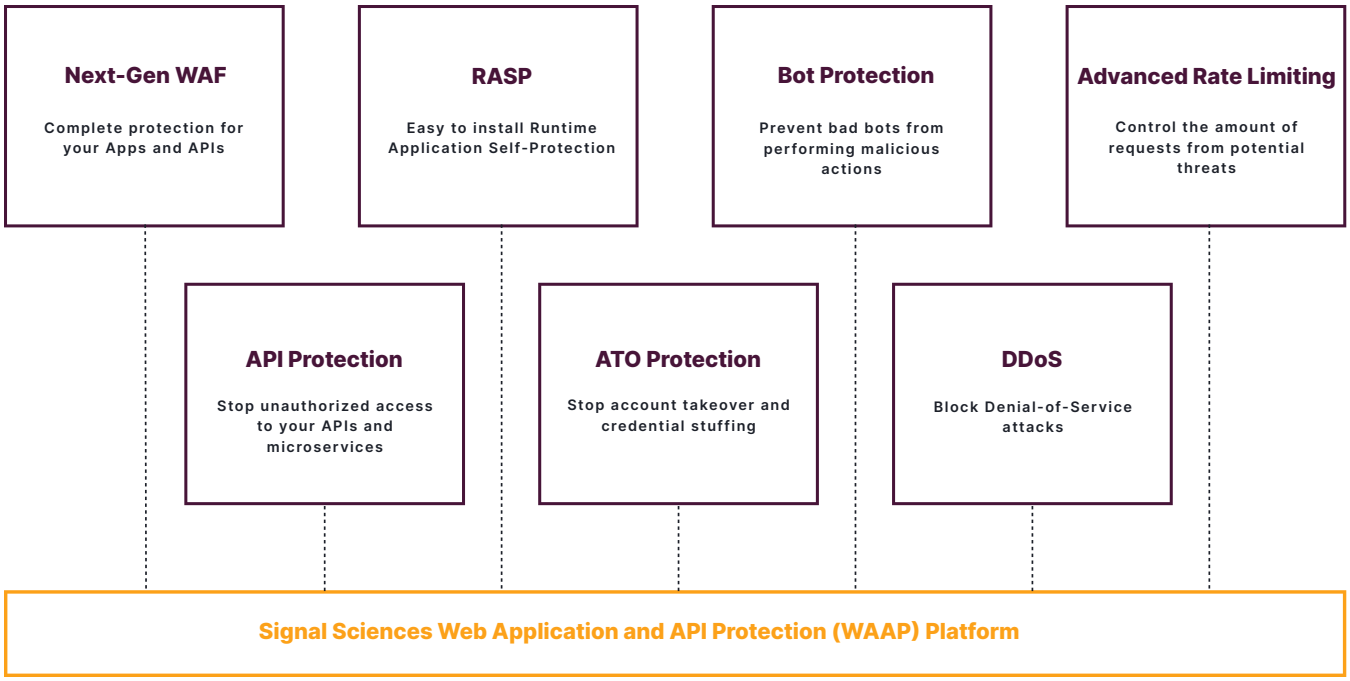
Measured in hours/days, not the months of legacy WAFs, so you can gain visibility quickly and stop web layer attacks automatically.

Cost

Significantly lower TCO than legacy WAF solutions with no managed services tuning fees.

Our web application security platform secures critical apps, microservices, and APIs no matter where they're deployed, providing security coverage for your organization's entire application portfolio.

The SaaS-based architecture that powers our Web Application and API Protection platform is the foundation upon which other key protection capabilities secure applications in any environment, including multi- or hybrid-cloud. Built upon our patented agent-module pair that can be deployed in multiple patterns suitable for any application, our platform is an evolution of our next-gen WAF and RASP service offering. Providing comprehensive application and API protection that is fast and easy to deploy means our customers can protect their applications quickly and effectively against a broad range of security threats.



Our platform provides seven key capabilities that customers leverage to protect their business-critical apps and APIs.

Platform Benefits:

Uniform Coverage Across Datacenter and Cloud	Protection Against Advanced App and API Threats	Significant Budget Savings
• Architectural flexibility allows customers to leverage one control they can deploy regardless of language and infrastructure that development and operations teams choose to design and deliver software. • Native deployment options available for datacenter, cloud, containers, API gateways, service mesh and others. • One hybrid SaaS console provides a single management plane for policy enforcement, reporting, and integrating with security and application toolchains.	• Protects against not only classic OWASP Top 10 Attacks but also advanced web attacks. • Provides additional attack coverage against account takeover, bots, API abuse, DDoS, and more. • Advanced rate limiting offers application-specific protection while virtual patching enables ops teams to quickly address known vulnerabilities in web server operating systems.	• No expensive rule-tuning services required, period. • Fast time to value: be up and running in production in hours or days, unlike legacy web application firewalls that typically require months of tuning out false positives.

DevOps, SOC, and SIEM Toolchain Integrations

The best path to success for effective application and API protection is to provide the same baseline of security data to development, operations and security teams in the tools they're already using. That means real-time alerting into DevOps, SOC, and SIEM toolchains and enabling the ingestion of web application security telemetry into other security tooling for further investigation and analysis. Signal Sciences works with the industry's best tools and platforms to ensure it's easy for your teams to leverage our production security telemetry within your organization's current tools and processes.

Out-of-the-box technology integrations help teams make or continue their transition to modern development models and architectures. Our single-click integrations include the most common development and operations alerting engines, chat-ops, project management, and incident tracking systems.

Technology and Platform Integrations

Feed Integrations & Partners

Send and receive data from Signal Sciences.

DEVOPS TOOLCHAIN

Jira Software, slack, DATADOG, OpsGenie, VictorOps, Microsoft Teams, PagerDuty, PivotalTracker

SOC/SIEM

splunk>, Radar, CORTEX XSOAR, ArcSight, elastic, cisco, LogRhythm, RSA, McAfee

Platform Integrations & Partners

Run Signal Sciences on everything.

IAAS

Google Cloud, aws, Microsoft Azure

PAAS

HEROKU, Microsoft Azure, Red Hat OpenShift, vmware Tanzu

WEB SERVERS

NGINX, APACHE, Microsoft IIS, Apache Tomcat, IBM Cloud

CONTAINERS

kubernetes, docker, OPENSHIFT, Istio, envoy, MESOS

CONFIG MANAGEMENT

CHEF, ANSIBLE, puppet, SALTSTACK

> **"Getting Signal Sciences up and running is quick and easy. It was literally a five minute process.**

Robert Davis, Director of Cybersecurity, **Chick-fil-A**