The Keys to Securing Internal Apps Quickly When They Become External Facing

Enforce Zero Trust and Protect Your Apps

Internal business applications historically relied on being inaccessible without VPN access as a key security control. With the rise of Zero Trust and a work-from-home (WFH) work force, business critical internal applications are being placed outside of VPNs and DMZs. Many of these apps were built to be only internally accessible, so they often lack the security level of apps developed to be Internet facing. Customers use Signal Sciences to rapidly gain cost effective protection of these applications for three key reasons:

1. Gain security coverage over exposed internal applications

When an organization's security and IT team needs to protect internal applications suddenly made public-facing to effectively serve more users, Signal Sciences can provide advanced attack detection and prevention including:

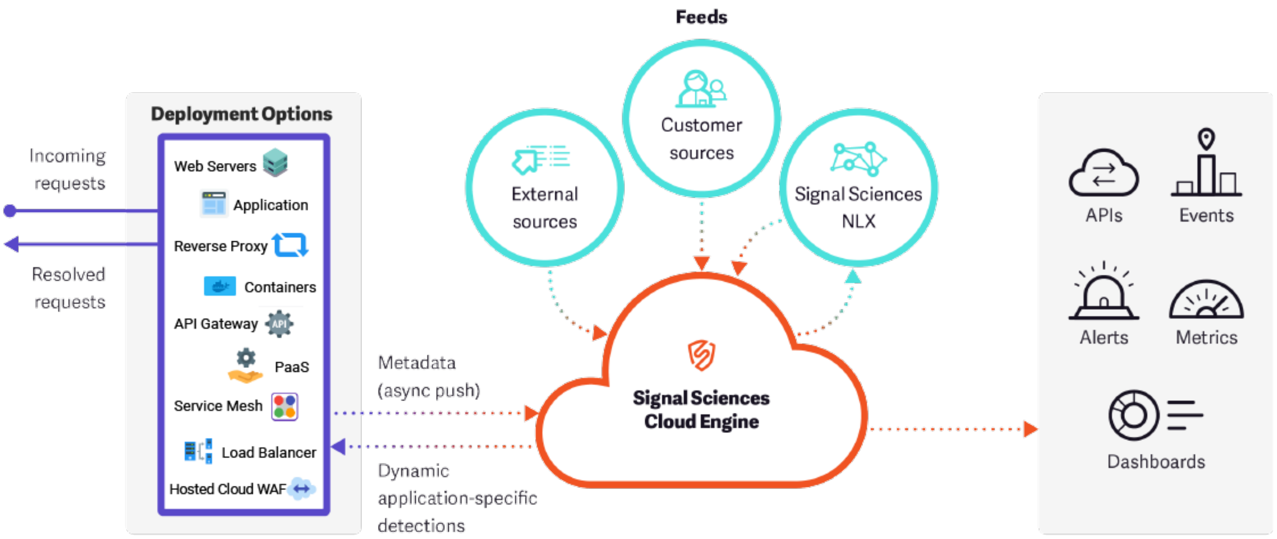
- **Employee account takeover (ATO) via credential stuffing.** While identity access management (IAM) solutions provide control over user credential usage, any application with an authentication flow is still a target for ATO attempts. Signal Sciences provides the ability to monitor for anomalous requests and block suspicious login attempts.
- **OWASP Top Ten injection attacks.** Many internal apps are not built to the same standard as external apps so stopping injection attacks without modifying the application is key.
- **Sensitive business logic abuse.** Business logic in previously internal apps is rarely protected against abusive and malicious behavior. For example, attackers will often attempt to exploit a lack of rate limiting to access sensitive data via guessing or enumerating identifiers such as financial record IDs. They may also attempt to gain access to sensitive HR or internal communication resources via brute force methods.
- **Instant virtual patching to address documented platform issues.** Previously internal applications are often the last to get patched in a network environment. Signal Sciences provides out of the box coverage for CVEs impacting major application platforms and frameworks so your applications can be protected the moment they become externally facing. Examples include published CVEs for widely used apps made public, including Apache Struts and vulnerabilities in Confluence.

> Finally a WAF that works without endless tuning and false positives! Signal Sciences was very easy to deploy and we immediately went into block mode without having to do any tuning and have not had false positives.
>
> —Director of Network Security Operations at $250M+ Professional Services Firm

2. Deploy web app protection *fast*

Given the often abruptness of internal applications becoming externally accessible, being able to deploy protection FAST is a critical requirement. With Signal Sciences, you gain comprehensive app protection with our flexible, quick deployment options that:

- **No agents required.** With the Cloud WAF deployment option there's no software to install: just a single DNS change and Signal Sciences Cloud WAF automatically inspects application and API traffic to block malicious requests without impacting legitimate traffic.
- **Provide comprehensive protection in under an hour.** With Signal Sciences you can be blocking application attacks in production, on average, in 60 minutes or less. Our fastest installations have occurred in under five minutes: customers get fast time to value by gaining coverage over application and API attacks without manual tuning.
- **Protect your apps in any infrastructure.** Installs in any infrastructure, including cloud, on-premise, containers or hybrid environments.



Signal Sciences installs quickly in any infrastructure where you run your apps. Our flexible deployment options enable organizations to protect public, Internet-facing apps quickly: the average installation time is an hour and can be as fast as a few minutes. Our Cloud WAF deployment does not require any software installation and offers all the features and protective benefits of our other deployments.

3. Save overhead costs

Typically the only way to protect newly-external apps in the past was to deploy a content delivery network (CDN) or full load balancer in front of them, but that approach introduces massive cost overhead because you're paying for CDN and/or load balancer functionality that simply isn't needed for applications initially intended for internal users. But Signal Sciences eliminates the costs that legacy WAF appliances require to get value from them:

- **Get standalone coverage without having to pay for needed services like a CDN or load balancer.** With Signal Sciences you can gain cost effective protection for sensitive applications and APIs without paying unnecessary overhead fees for a CDN or load balancer that simply aren't needed for internal applications that generate low traffic but allow access to highly sensitive data.
- **No FTE staff dedicated to WAF maintenance.** Security teams don't have time to manage and tune false positives given the scale of internal applications. Due to our modern approach to detecting and blocking attacks, no Signal Sciences customer has had to dedicate a FTE to rules maintenance and tuning out false positives.

Average Managed Services Fees

Signal Sciences	Other WAF Vendors
$0	$50-250K

> Signal Sciences is incredibly fast to implement and powerful to use. We were able to get up in running in a matter of minutes. Unlike traditional WAFs, Signal Sciences has very little overhead in terms of time or effort and returns an exponential impact for securing our organization.
>
> —Senior Manager Of DevOps at $30B+ Financial Services Company

The World's Top Companies Trust Signal Sciences

DOORDASH DATADOG DUO vimeo

tenable SHINOLA DETROIT one medical UNDER ARMOUR

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

Datadog

Webhooks

Splunk

SIEM/SOC tools via APIs

+ MORE