Integrating the Ambassador Edge Stack with Signal Sciences

With a new integration between the Ambassador Edge Stack and Signal Sciences next-gen Web Application Firewall (WAF), platform teams can now further protect cloud-native applications built on Kubernetes while enabling developers to independently deploy microservice improvements.

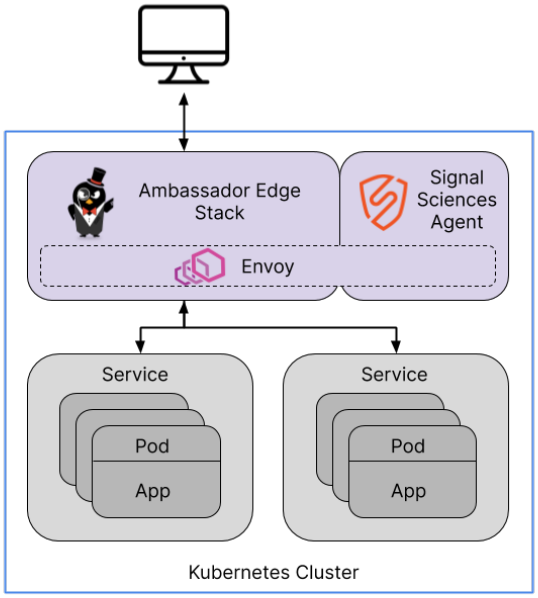
Why Is Routing Management Different with Microservices?

Today, organizations leverage a microservices architecture to revolutionize their products and improve user experience with faster, more frequent releases. In order to realize the full value of microservices, development teams need the ability to build, test, and deploy services without centralized, operational control. However, security policies need to be enforced centrally. Especially with the shift to Kubernetes, more services are exposed at the edge, which increases attack vulnerability at the surface. Securing applications and protecting against malicious attacks is inherently more difficult while also trying to decentralize microservice deployments and edge policy configurations. API gateways and web application firewalls are commonly used tools to address these concerns.

Integrating the Ambassador Edge Stack with Signal Sciences WAF

The Ambassador Edge Stack integration with Signal Sciences next-gen WAF empowers developers to adhere to an organization's security policies while supporting their ability to build and deploy services fast. Teams can feel confident that the right security measures are put in place—like authentication, rate limiting, TLS encryption, and now WAF configuration—to protect against malicious threats without impacting developer productivity.

This integration makes it easier for organizations to configure a next-gen WAF for all incoming traffic at the cluster edge through their API gateway. With the integration, a filter and plug-in enable teams to send the metadata of all incoming requests to the WAF from the Ambassador Edge Stack. Depending on whether the WAF allows or denies the request, the Ambassador Edge Stack will either allow or block traffic from entering the cluster.



Why Do You Need a Next-Gen WAF?

Signal Sciences next-gen WAF provides superior protection for applications and APIs by delivering the following benefits over legacy appliance-based WAF solutions.

Scalability on Demand

Signal Sciences protects modern applications and APIs across different stacks and clouds, allowing organizations to scale up and down based on demand. Unlike legacy WAFs, our elastic technology runs anywhere without adding the overhead of configuring and deploying new instances and rule sets. Scaling is vastly simplified: your teams don't have to write new rules when deploying new apps or updating existing ones.

Protection Without Impacting Performance

Signal Sciences Cloud Engine currently protects over 40 thousand sites and 1.6 trillion requests per month, and has protected the websites for big events like the Super Bowl, the United States presidential election, and Black Friday for retailers, with no noticeable impact on quality of service. Our lightweight agents run wherever you run Ambassador, without requiring an additional network hop like appliance-based WAFs. The operational metrics on our dashboard show that the WAF introduces only minimal latency, on average just one to two milliseconds.

Advanced Threat Coverage

Customers with traditional WAFs are rightfully wary about the high false positive rates that come with rules defined by regular expression, and often never deploy in blocking mode. Additionally, customers need more protection for their APIs, microservices, and other web properties. 95% of customers run in blocking mode because they are confident in our threat protection from OWASP Top 10, account takeover, bots, volumetric attacks, and more. For deeper, more customizable blocking options, Signal Sciences Power Rules give customers the flexibility to adapt blocking rules to their own environment based on a number of criteria.

Why Do You Need an Edge Stack?

The Ambassador Edge Stack allows developers to easily expose, secure, and manage traffic to your Kubernetes microservices of any type.

Self-Service Model

The Ambassador Edge Stack enables platform teams to provide edge-as-a-service to application developers, improving agility while ensuring best practices are followed. This frees platform teams from ticket management and allows developers to work with more autonomy and velocity to release better products.

Comprehensive Edge Management

With all the functionality of a cloud native API gateway, the Ambassador Edge Stack provides the broad spectrum of functionality necessary to support edge microservices today, reducing complexity and overhead. The variety of supported integrations and tools enables each developer the flexibility to choose the right technologies for their microservice. The Ambassador Edge Stack includes load balancing, authentication with popular IdPs (Keycloak, Azure Active Directory, Okta), rate limiting for DDoS attacks, TLS encryption, observability with Prometheus and Grafana, distributed tracing with Zipkin, and integrations with service meshes (Istio, Consul, Linkerd).