Signal Sciences

Signal Sciences Next-Gen WAF Support for Envoy

Application, API and Microservices Protection at Scale

SUMMARY

Signal Sciences Next-Gen WAF support for Envoy provides application-layer security for all applications, APIs, and microservices proxied with Envoy.

Signal Sciences Next-Gen WAF support for Envoy provides application-layer security for all applications, APIs, and microservices proxied with Envoy. Deployable without code changes, Signal Sciences enables protection for north-south and east-west traffic between microservices against application-layer attacks.

Commonly used as a proxy within a service mesh deployed in Kubernetes, Envoy helps ease the transition to, and operation of, cloud-native architectures by managing interactions among microservices to ensure application performance.

Unlike legacy WAFs that require rule sets for each service, application, or API behind the WAF, Signal Sciences SmartParse technology dynamically detects malicious payloads without any rule definition or regular expression pattern matching. As a result, organizations instantly gain scalable protection and increased visibility for their cloud-native applications.

Comprehensive Visibility at Scale

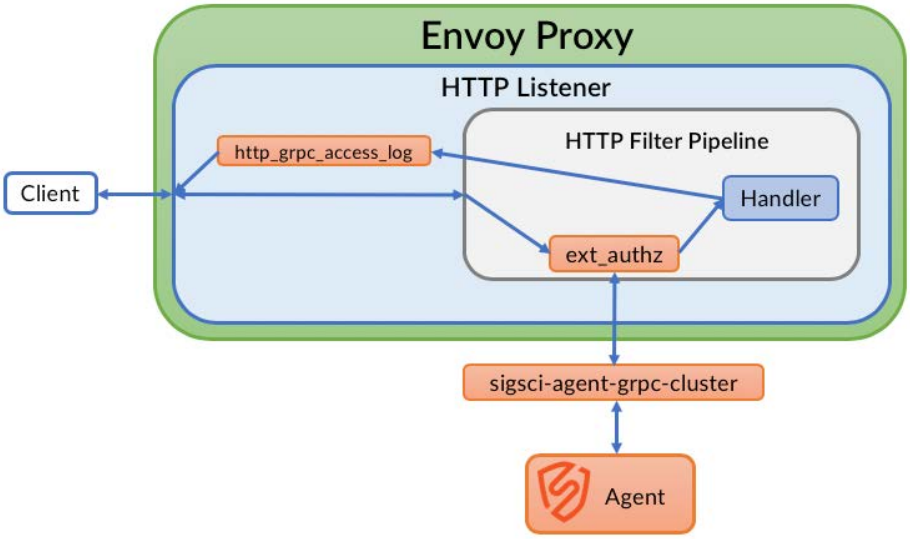
As organizations move to cloud-native applications and services, Signal Sciences makes it effortless to achieve advanced Layer 7 security and comprehensive visibility at scale for Envoy, a cloud application networking technology. With this integration, Signal Sciences provides customers utilizing Envoy even greater flexibility to implement web application and API security for any app or service on any infrastructure.

KEY BENEFITS

- **See:** Organizations instantly gain scalable protection and increased visibility for their cloud-native applications.
- **Secure:** Protects north-south and east-west traffic between microservices against application-layer attacks.
- **Scale:** Deploys without code changes.

Integrating Signal Sciences with Envoy

When acting as a Front Proxy, Envoy load balances public north-south traffic from the Internet—that's HTTP traffic that needs to be protected against Layer 7 attacks. The module in our patented agent-module pair forwards requests to the agent, which performs detection and decisioning on the web requests it inspects. The benefit of this split approach is that Signal Sciences is fail-open, which is important to gain credibility as a security service with DevOps and operations teams. Our engineering team designed our integration so that Envoy acts as the "module" forwarding requests to our agent for web request inspection.



Signal Sciences Protects All Services Running Behind Envoy

By deploying Signal Sciences on Envoy at the edge, all services running behind Envoy are protected. Unlike a legacy WAF that would have to define rulesets for each service, application or API behind the WAF, Signal Sciences SmartParse technology detects malicious payloads dynamically without any rule matching. Our architecture provides scalability that is orders of magnitude greater than individually tuning rulesets for "n" number of services and applications deployed behind the proxy to provide application, API and microservices protection at scale.

Any App

Cloud, Containers, PaaS, and Serverless

Web Servers and Languages

API Gateways and Proxies

Any Attack

OWASP Top 10

Application DoS

Brute force attacks

+ MORE

Any DevOps Toolchain

Slack

Splunk

PagerDuty

SIEM/SOC tools via APIs

Datadog

Webhooks

+ MORE