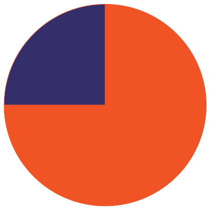
Securing Containers at the Speed of Innovation

Containers and deployment orchestration frameworks are becoming the foundation for CI/CD pipelines to rapidly deploy the apps, APIs and microservices that power the modern web: they provide the ability to add capacity that scales, orchestrate zero-downtime deployments, and provides an infrastructure fit for microservices and APIs.



By 2022, more than 75% of global organizations will be running containerized applications in production[1].

Driven by the need to scale their applications rapidly for competitive advantage and serve rapidly expanding customer bases, software teams now often rely on containers and container orchestration tools like Kubernetes to release applications at increasing velocity. Despite rapid adoption, security concerns about container usage are also prevalent: 43 percent of developers say security challenges block their container adoption[2]. While extremely flexible and fast, containerized applications are also targets of malicious attackers.

Secure Containerized Apps and Increase Velocity

Signal Sciences patented agent runs natively in any cloud, data center, or container, allowing for several flexible deployment options at the code layer, web server, API gateway, or cluster ingress. Our architecture was designed for easy deployment of our agent as part of the container running your application, or as a Docker sidecar, regardless of the underlying server instance OS or code language. Installation is simple, allowing you to secure your applications, APIs, and microservices in minutes.

Signal Sciences protects containerized applications in production and empowers CI/CD pipelines by:

- Inspecting and blocking malicious web requests to containerized applications and workloads
- Providing fast time-to-value with immediate visibility into both North-South and East-West web request traffic
- Embedding application security capabilities within containers and automated deployment tools like Kubernetes
- Provides superior advanced attack prevention that legacy WAF appliances cannot match

[1] "Top Emerging Trends in Cloud-Native Infrastructure" - Gartner Research, May 2019

[2] Now Tech: Container Security, Forrester Research Q4 2018

How We Do It: Delivering Container Security at Scale

Our patented agent and module operate in customers' on-premise or public cloud infrastructure. They pass web request meta data to our Cloud Engine for enhanced intelligence that provides web request context. The module is not needed when the Signal Sciences agent is configured to operate in Reverse Proxy mode. As a Reverse Proxy, the agent inspects incoming web requests before sending them upstream to the application.

Where and how you run Signal Sciences in Docker and Kubernetes depends on your infrastructure. There are three main layers where customers can install Signal Sciences:

- **Kubernetes ingress controller:** used by customers with an ingress controller (e.g., NGINX, HAProxy, Envoy) who want to centralize the security of all apps residing behind the ingress controller
- **The service or web server layer**: used when there is no ingress controller or the customer runs a load balancer to front traffic but can't install there for any given reason (note: Signal Sciences can install at the load balancer, but customers' requirements sometimes prevent them from doing so)
- **The application code layer**: installing here enables application teams to control the installation themselves.

Methods

Within each of the layers noted above, Signal Sciences deployes in conjunction with Kubernetes in any of the following four ways:

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

A total of 12 installation options match the flexibility that containers and Kubernetes offer software teams. Additionally, the Signal Sciences agent can deploy as a Docker sidecar, which legacy WAFs cannot. All these install options offer precise instrumentation of web requests without the pitfalls of other WAF and RASP approaches. See something in the raw data that you'd rather delete? Submit a support request for Signal Sciences automated tools to go through and scrub our database of your requested field.

Ultimate Flexibility to Secure Applications and Microservices

With Signal Sciences, you have ultimate flexibility to secure your applications and microservices quickly no matter how your software teams leverage containers with Kubernetes. Our customers can protect their apps on day one while ensuring their applications remain secure in the future, even if their app deployments via Kubernetes change.