radware

Data Sheet

Secure Data and Applications Running in a Service Mesh

As business enterprises are looking to optimize and accelerate their continuous integration and continuous delivery (CI/CD) pipeline, old blind spots are exposed and new blind spots are created, leaving data integrity at risk. SQL injections, cross-site scripting, access violations, data leakage and service disruptions don't go away when running applications in a service mesh architecture. Therefore, security must adapt to and blend in with this new ecosystem.

Radware Kubernetes Web Application Firewall (WAF) enables secure delivery of applications at the speed of development without compromising agility. It is designed to fit the Kubernetes orchestration system in service mesh architecture, providing market-leading application security as well as the advanced automation, autoscaling and elasticity required by today's development and operations (DevOps) and security teams.

MARKET-LEADING SECURITY TECHNOLOGY

Positive and negative security models combined, autolearning and behavioral policies, and data leakage prevention. Recommended by NSS Labs and certified by ICSA Labs

COMPREHENSIVE REPORTING AND ANALYTICS

Visibility to development, security and operations (DevSecOps) + security teams via integration with common tools and platforms such as elastic Kibana, Grafana and more

DEVSECOPS READY: SCALE, AUTOMATION & ELASTICITY

A Kubernetes controlled service: application security grows and scales with Kubernetes pods, including manually configured and autogenerated policies

ADVANCED AUTOMATION

Perfectly tailored to integrate into a CI/CD pipeline and facilitate security provisioning of new services and applications

How Radware's Kubernetes WAF Keeps Your Kubernetes Environment Agile and Secure

Unmatched Security

- Combining positive and negative security models
- NSS Labs recommended and ICSA Labs certified technology
- Zero-day attack protection
- Data leakage prevention
- Full coverage of the OWASP Top 10 vulnerabilities

At the Speed of Business

- Auto-policy generation and optimization engine
- CI/CD pipeline integration
- Scalability and elasticity
- High availability
- Visibility through integration with common tools
- Local management and reporting interface

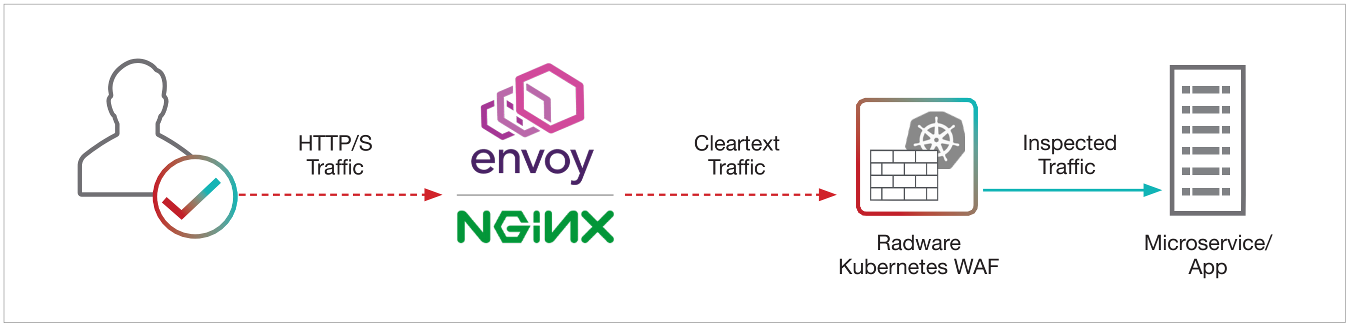

Figure 1: Radware's Kubernetes WAF deployed as a reverse proxy

Key Features

Web application security in front of each Kubernetes pod to protect data integrity

Positive and negative security models to maximize protection against known and unknown attacks

Fits into a Kubernetes ecosystem meeting the required level of automation and scale for a seamless integration and operation

Reverse proxy deployment so security is enforced on every transaction; ability to mask data, encrypt cookies and modify responses

TLS termination allows single termination only at the host level; no need to manage multiple SSL certificates across different parties

Minimal footprint with light enforcement agent in front of each pod; external management platform

Granular visibility serving both security and DevOps teams

- Security events and policies
- Operations: application telemetry, network stats, performance and latency results
- Interoperability with various open-source visibility platforms

This document is provided for information purposes only. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law. Radware specifically disclaims any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The technologies, functionalities, services, or processes described herein are subject to change without notice.