Rohde & Schwarz Cybersecurity

R&S®TRUSTED APPLICATION FACTORY

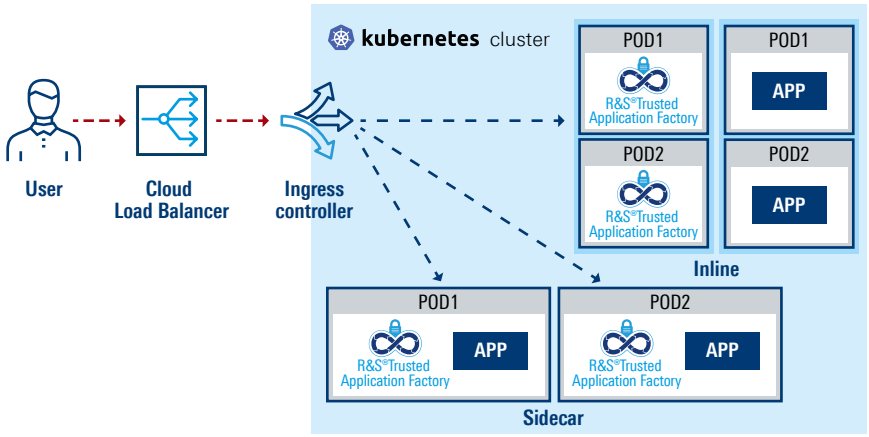
A cloud native application protection solution to shift security left for your microservices and their APIs.

► Use our containerized technology to blend homogeneous security, with agile release cycles, for your application development.

Modern teams are going cloud native by moving to microservices based architecture. With the usage of microservices, east-west traffic is growing too. It is critical to secure this lateral traffic to reduce available attack surface in internal systems. Moreover, attacks highlighted in OWASP Top 10 are still relevant for cloud native applications. In addition, some underrated attacks like credential stuffing also need to be taken into account. Integrating a security solution into your CI/CD toolchain involves human resource costs. Many companies rely on powerful tools like SAST, DAST and SCA. However, these tools partially cover the OWASP Top 10 and do not ask for precise information from developers to describe an application/API easily. SAST gives rise to many false positives and cannot determine new runtime vulnerabilities. DAST and SCA help spot many vulnerabilities but it can be a nightmare for companies to handle them all. Hence, these security testing tools are not sufficient anymore to ensure the security of your applications, especially against zero-day attacks.

Product Flyer
Version 01.00

ROHDE&SCHWARZ
Make ideas real



SUPPORTED ENVIRONMENTS		
Cloud		
AWS	GCP	Microsoft® Azure
Containers		
Docker	Kubernetes	OpenShift
Service mesh		
Istio	Ambassador	Consul
Insights		
Syslog	Logstash	Fluentd
CI/CD tools		
Gitlab	Jenkins	CircleCI

R&S®Trusted Application Factory has a simple architecture designed for Kubernetes and more.

Solution overview

In this era of Security as Code, R&S®Trusted Application Factory is an excellent way to expedite digital transformation in your overall infrastructure. The solution automates everything in your DevOps ecosystem – from development, code commit, security testing to production and improves time-to-market. The ability to integrate security configuration close to the application, allows DevSecOps teams to address challenging security concerns early on in Build phase, complementing their SAST/DAST approach. It displays value upfront by testing the application in a preproduction environment, to protect it during run phase. The solution lets you prioritize, track and expedite the time, to virtual patch new vulnerabilities by creating custom rules. Developers will have more time now to do a proper fix as per their schedule.

Reduces complexity with standard configuration file

This containerized solution is implemented directly within the CI/CD pipeline with the already existing tools like Gitlab, Jenkins etc to simplify collaboration. Achieving interoperability within the CI/CD domain is key. Same formats (as YAML, GO like), form factor (Docker images), languages and concepts are used which results in easy management, low TCO and no new learning curve for developers.

Simplifies approach with proactive engines and whitelisting

The solution activates security engines built on 20 years of expertise, rate limiting, and bot mitigation capabilities to respond to OWASP Top 10, zero-day attacks, DoS and threats like credential stuffing that do not exploit CVEs. Built with API first mindset, it allows OpenAPI file enforcement to secure both north-south and east-west traffic flow.

Increases ROI by automatically adapting to app traffic

The solution is deployed as a micro-WAF within the application enabling users to scale up or down at the same time as the application using their orchestrator, in Kubernetes, OpenShift or Docker clusters. Thus, it can automatically adapt to the load of the application. This diminishes costs of resources and augments return on investment.

Improves security with context enriched description

The solution along with context description (such as used persistence type, programming language, server OS, data format) is integrated in a configuration file close to the application code. This keeps security up to date and aligned with application's version. Security policies can be adapted automatically by invoking relevant security engines.

Optimizes costs by preventing false positives, data loss

R&S®Trusted Application Factory corrects vulnerabilities in the easiest way possible. It creates exceptions by automatically detecting false positives in a preproduction environment and limits false positives in production. It can detect sensitive data with outgoing filtering capabilities acting on the backend response in order to prevent data loss and ensure compliance.

Develops agnosticity with rapid and flexible deployment

R&S®Trusted Application Factory can be rapidly deployed both on premises and on the cloud (both private and public) with minimal effort. The security engines reside on premise, while we handle other functionalities in a SaaS environment. The form factor ensures high availability and performance of applications for the users.

Rohde&Schwarz Cybersecurity GmbH
Muehldorfstrasse 15 | 81671 Munich, Germany
Info: +49 30 65884-222
Email: cybersecurity@rohde-schwarz.com
www.rohde-schwarz.com/cybersecurity

Rohde&Schwarz GmbH&Co. KG
www.rohde-schwarz.com

PD 3608.8563.32 | Version 01.00 | July 2021 (sch)
R&S®Trusted Application Factory
Data without tolerance limits is not binding | Subject to change

3608856332

3608.8563.32 01.00 PDP 1 en