Red Hat **Partner Connect**

Portshift combines containers and service mesh security

Red Hat Software Partner

portshift

> "Having Portshift's information-rich view of containers in real-time will be exceedingly important in 2020 as more determined hackers continue their efforts to attack earlier in the development process in order to exploit vulnerabilities before they are addressed by DevSecOps."

Zohar Kaufman,
Co-Founder and VP R&D , Portshift

Red Hat
Technology Partner

Red Hat
Certified Technology

facebook.com/redhatinc
@RedHat
linkedin.com/company/red-hat

Portshift provides application runtime security

Portshift is an identity-based cloud workload protection platform that provides applications runtime security. Portshift enables real-time visualization of workloads, and the enforcement of communication rules based on applications attributes that are associated with their development and deployment cycles. Portshift enables DevOps teams to orchestrate security as part of their day-to-day job. Portshift's unique model introduces an agentless security framework that is decoupled from network and operations, allowing for accelerated software delivery at any scale.

Executive Summary

Portshift prevents untrusted code from running and ensures that containers remain immutable. You can monitor and control Red Hat® OpenShif® clusters activity in real-time, based on custom policies and machine-learned policies controller. Alert, detect or block malicious communications or compromised pods without killing or pausing workloads, ensuring business continuity and utmost security.

Product Profile

Portshift containers runtime security platform, is an agentless solution providing holistic security to running containers in OpenShift environments. Portshift's controller protects containers (e.g. known vulnerabilities, authorized deployments settings), de-ployments and containers' routes (Kubernetes services) with a seamless deployments and declarative intuitive policy. Portshift management is a SaaS application that eliminates the need to deploy and manage or scale on-prem instances. Complemented by continuous integration and continuous delivery (CI/CD) plugins, Portshift offers a seamless and scalable runtime security experience.

Product Benefits

- Portshift offers seamless runtime security with agentless security offering, containers deployment authorization based on CI/CD attributes (vulnerabilities, image signing/verification, deployments metadata) with intuitive and granular pod security context policies.
- Declarative network policies enforce consistent and granular security policies inside the cluster and outside the cluster connecting to on-prem or PaaS services.
- Seamless deployment with SaaS management and automated Kubernetes deployment.
- A managed policy engine which detects and offers runtime remediations to newly discovered threats.

OpenShift Containers runtime security:

- Agentless runtime security
- Seamless integration with SourceToImage (S2I)
- Native integration with Istio/Service mesh: simplified network policies inside/outside OpenShift clusters

Use cases

- Complete visibility on all workloads and their security context.
- Workload policy authorization based on its attributes and security context collected during CI/CD phase and pre-runtime deployment.
- Comprehensive, declarative and simplified network policies inside and outside the clusters allowing consistent security for all application resources.
- Scalable and automated "0 trust network" implementation in the cluster.

> "The global deployment of Kubernetes by organizations continues at a rapid pace, making it imperative that cloud-native identity-based protection is in place. DevOps and DevSecOps managing the security in these operationally-significant Kubernetes environments are moving to centralize security."
>
> **Ran Ilany,**
> CEO and co-founder, Portshift

Learn more

Company: Portshift info@portshift.io www.portshift.io

About Portshift

Portshift's identity-based security platform delivers runtime security across OpenShift clusters, securing applications from CI/CD pipeline to runtime deployments, leveraging unique pods security controls and service mesh policies to secure internal and external network traffic.

About Red Hat

Red Hat is the world's leading provider of enterprise open source software solutions, using a community-powered approach to deliver reliable and high-performing Linux, hybrid cloud, container, and Kubernetes technologies. Red Hat helps customers integrate new and existing IT applications, develop cloud-native applications, standardize on our industry-leading operating system, and automate, secure, and manage complex environments. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500. As a strategic partner to cloud providers, system integrators, application vendors, customers, and open source communities, Red Hat can help organizations prepare for the digital future.

facebook.com/redhatinc
@RedHat
linkedin.com/company/red-hat

North America
1 888 REDHAT1
www.redhat.com

Europe, Middle East, and Africa
00800 7334 2835
europe@redhat.com

Asia Pacific
+65 6490 4200
apac@redhat.com

Latin America
+54 11 4329 7300
info-latam@redhat.com