Kubernetes Runtime Security

Identity-based runtime protection for containerized microservices

www.portshift.io
Portshift’s innovative workloads protection for containerized applications starts at the CI/CD pipeline.

The Portshift universal CI/CD pipeline plugin creates a unique identity for each image artifact. This is used to enforce runtime security policies, when these images are built as containers in Kubernetes clusters. These policies prevent deployment of unknown or vulnerable images in your cluster. Portshift network policies also govern the connections of your microservices. They detect malicious or non-authenticated connections and alert or block them.

Portshift leverages the Istio service mesh for large scale seamless deployment of enforcement elements inside running clusters and production environment. A learning policy engine automates the process of creating security policies together with optional mutual TLS encryption between pods, and services. Portshift automates the deployment and configuration of Istio service components. The Portshift agent utilizes the Istio Envoy proxy to achieve micro-segmentation and application isolation, with a user-friendly, highly intuitive interface.

Automated Policy Engine

Seamlessly integrated within Kubernetes and the service mesh, Portshift automates runtime protection. The Portshift policy engine creates a communication policy for all pods and external resources that communicate with them. Portshift network policies use an intuitive human-readable language to authorize connections within Kubernetes clusters. The Portshift automatic policy-engine ("Policy Advisor") analyzes the Kubernetes services (and connections), and suggests the most operationally efficient and secure network policy.

Identity-Based Workload Protection, from CI/CD Pipeline to Runtime

Portshift offers a zero-trust architecture with identity-based runtime protection. First, it creates a unique identity for each workload, early in the CI and CD pipeline. It then uses these identities to enforce runtime security policies on clusters, preventing unauthorized workloads running, and communicating with legitimate ones. Portshift immediately identifies unauthorized communications, and alerts or blocks them.
Authenticated Communication at Runtime

Portshift Unleashes the Power of the Service Mesh Architecture

The Istio service mesh offers a number of security, reliability, and efficiency benefits that can help your organization to manage cluster traffic, and increase network stability. When you use Portshift, it serves as the key to unlock the benefits of Istio, leveraging it as the vehicle for uniquely frictionless, rules-based, cluster security. Portshift deploys and manages Istio components inside your cluster, giving you the operational benefits. You don’t have to put any effort into installing, integrating, or implementing it.

Container Segmentation

Portshift provides the most effective runtime protection, using Istio to configure micro-segmentation, and deliver a highly intuitive interface that gives you complete control over security rules and policies for your Kubernetes clusters. With Portshift, every microsegment is a separate entity, with its own identity. Runtime security policies control your microsegments natively, ensuring your components only run as you intend them to.
Seamless integration with your stack, across the cloud native ecosystem.

In today’s devops world, the trend is towards cloud-native applications, micro-segmented across containers, clusters, and even platforms. With Portshift, you can keep up with this pace and apply a single security solution that works across platforms, but doesn’t get in the way of your devops. Portshift is designed for Kubernetes clusters, on a number of orchestration platforms. Portshift helps to secure and protect your multi-cluster deployments, providing you runtime visibility and intuitive policy control whether you are using native Kubernetes or managed services such as AKS, GKE, EKS. Enterprises that use Rancher or Red Hat OpenShift to build, deploy, and manage their containers also use Portshift to provide complete security protection for their environments.

Portshift is Platform-Independent

Enterprises that use Rancher or Red Hat OpenShift to build, deploy, and manage their containers also use Portshift to provide complete security protection for their environments.

Use Cases

Istio Service Mesh Expansion: Connecting Kubernetes Clusters with VMs/Cloud PaaS Services

See how Portshift solves the use case of connecting external resources with service-mesh. Service-meshes fit nicely and smoothly in containerized microservices environment which use orchestration such as Kubernetes, Openshift, and Rancher, which quickly adopt and support the service mesh concept in general and Istio in particular. However, many applications use additional resources which are not containerized, not managed by containers Orchestrators, but interact externally with the clusters microservices.

Advanced Service Mesh Communication: Secure Multi-Cluster Connectivity

See how Portshift solves service mesh multi cluster communication securely. Service-meshes fit nicely and smoothly within a Kubernetes clusters. The service mesh control plane manages the services communication and the workload identities. However, when traffic needs to pass between clusters and the services and workloads information needs to be federated the challenges starts. Learn how Portshift uniquely provide a secure communication between clusters.

Portshift delivers Kubernetes run-time security. Our innovative digital identity-based solution creates a unique, signed identity for each workload at the CI/CD pipeline process, that is than used to enforce run-time security policies. Our mission is to enable DevOps, Security and Operations to team up and utilize our identity-based workload protection for continuous security of their cloud-native applications. Portshift leverages Istio service-mesh, and Kubernetes to provide seamless run-time security. When you use Portshift, it serves as the key to unlock the benefits of Istio, leveraging it as the vehicle for uniquely friction-less, rules-based cluster security. Portshift fully manages Istio, generating and applying the logic to configure security rules. You don’t need to put any effort into installing, integrating, or implementing it.