WhiteSource

WhiteSource for Containers

DataSheet

The Challenge

Containers are rapidly gaining popularity as microservices, boosting software development teams agility and helping them to deploy faster.
However, containerized environments are very complex, with multiple fast-changing components and layers.

Working with containers requires a different set of tools to ensure all security issues are covered in every stage of the development lifecycle, in the containers and in the software deployed on them.

The Solution

WhiteSource for Containers offers a holistic approach for open source components management throughout the container development lifecycle. It provides complete visibility and control throughout the container development lifecycle by automatically detecting all open source components in your container images and containers and by enforcing policies automatically during development and production.

WhiteSource for Containers offers native integration to all environments along the way, including all CI servers, container registries, and container orchestration tools like Kubernetes.

With You Every Step of The Way
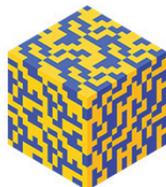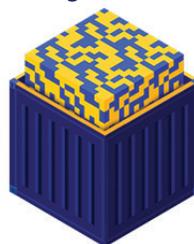
Development → **Build** → **Container Registry** → **Deploy**
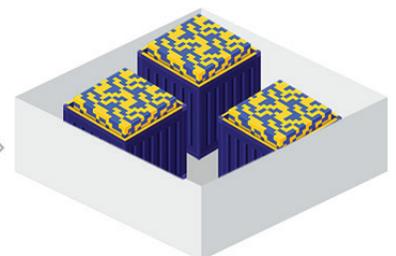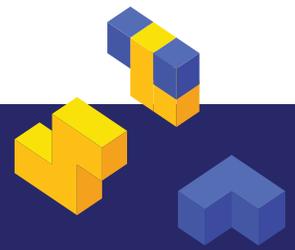
Top Benefits

1 Automatic Policy Enforcement

Initiate workflows for automatic approval and remediation upon detection of vulnerable or non-compliant components throughout the containers life cycle. You can even set-up safeguards like blocking production.

2 Native Integrations to Container Registries

Track vulnerabilities in file systems, installed packages, image layers and handled archive files without having to manually download and scan containers or images. WhiteSource for Containers supports all Container Registries: Docker Hub, Amazon ECR, Azure Container Registry, Google Container Registry, and JFrog Artifactory.

3 Risk-free Kubernetes Deployment

The Kubernetes agent runs silently in the background as a lightweight pod in the production cluster, automatically scanning any image deployed to production. The agent alerts on new vulnerabilities and enforces policies in real time, even after the software has been released to the market.

Product Specifications

Languages	Over 200 programming languages
Container registries support	Docker Hub, Amazon ECR, Azure Container Registry, Google Container Registry, JFrog Artifactory and GitHub Packages
Kubernetes agent	Kuberentes lightweight deployment, with configurable performance requirements
Deployment options	All three main cloud providers as a managed solution: Google Cloud, AWS, Azure - GKE, AKS, EKS, as well as full support for non-managed clusters
Linux Distributions	Debian, Arch Linux, CentOs Alpine
Kubernetes support	Kuberenets version 1.10 or higher
Reporting	Designated vulnerabilities report in WhiteSource and a designated dashboard
API	Full support, including new designated calls for Kubernetes data model
Installation	Quick and easy installation for Kubernetes using Helm (Kubernetes Package manager)

Kubernetes Dashboard

WhiteSource's Kubernetes Dashboard displays the comprehensive security status of your deployed resources in one dashboard. View vulnerabilities per pod or per severity, monitor the scan progress and analyze overtime alerts. Track your clusters' enforcement in real time and manage rejected resources.

Kubernetes Dashboard

Clusters	Pods		Reset View

Scan Progress

Last 7 days

2 Rejected Pods   12 Protected Pods

Vulnerabilities Distribution

Pod A
Pod E
Pod D
Pod C
Pod B

Vulnerabilities Severity

8

0   1

Low   Med   High

Alerts Overtime
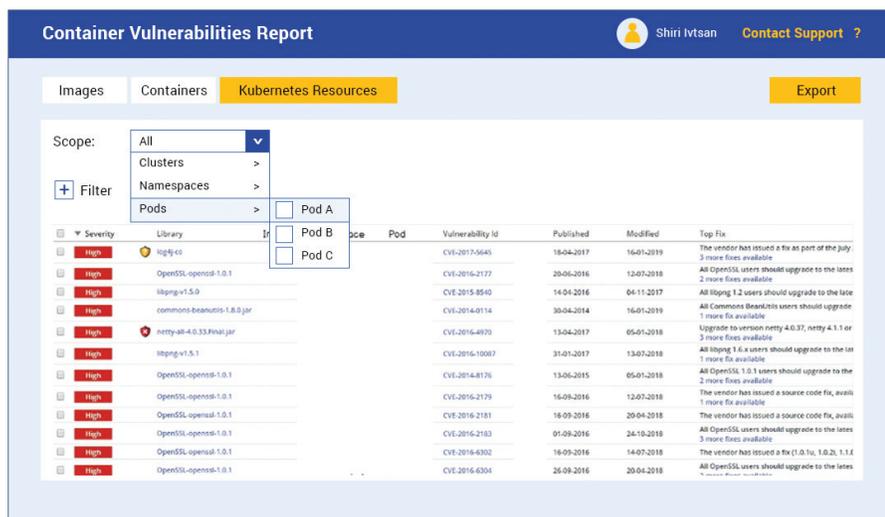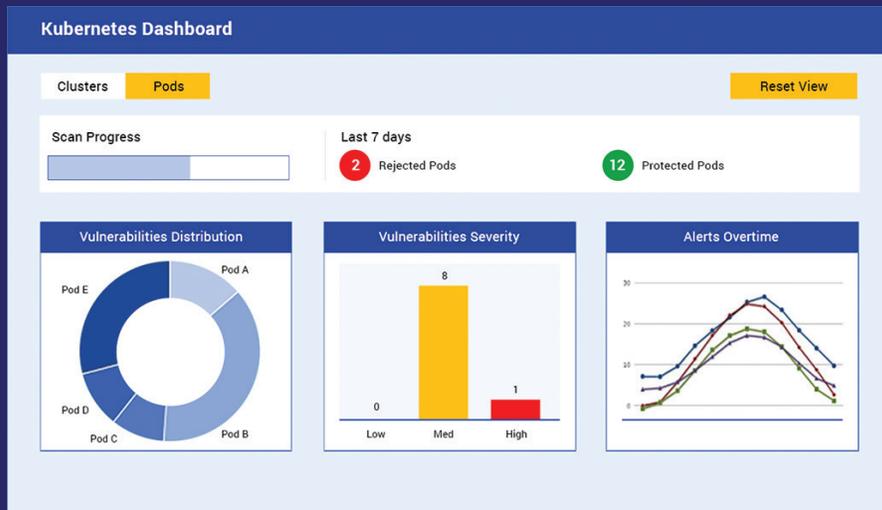
Container Vulnerability Report

The Container vulnerability report shows you a vulnerability breakdown for images, containers, or Kuberenetes resources. Track your vulnerabilities quickly and effectively, export to various formats or start a workflow based on the detected data.

Container Vulnerabilities Report

Shiri Ivtsan   Contact Support   ?

Images	Containers	Kubernetes Resources	Export

Scope: All

Clusters   >
Namespaces   >
Pods   >   ☐ Pod A
☐ Pod B
☐ Pod C

+ Filter

▼ Severity	Library	In	ce	Pod	Vulnerability Id	Published	Modified	Top Fix
High	log4j-co				CVE-2017-5645	18-04-2017	16-01-2019	The vendor has issued a fix as part of the July. 3 more fixes available
High	OpenSSL-openssl-1.0.1				CVE-2016-2177	20-06-2016	12-07-2018	All OpenSSL users should upgrade to the lates 2 more fixes available
High	libpng-v1.5.0				CVE-2015-8540	14-04-2016	04-11-2017	All libpng 1.2 users should upgrade to the late
High	commons-beanutils-1.8.0.jar				CVE-2014-0114	30-04-2014	16-01-2019	All Commons BeanUtils users should upgrade 1 more fix available
High	netty-all-4.0.33.Final.jar				CVE-2016-4970	13-04-2017	05-01-2018	Upgrade to version netty 4.0.37, netty 4.1.1 or 3 more fixes available
High	libpng-v1.5.1				CVE-2016-10087	31-01-2017	13-07-2018	All libpng 1.6.x users should upgrade to the lat 1 more fix available
High	OpenSSL-openssl-1.0.1				CVE-2014-8176	13-06-2015	05-01-2018	All OpenSSL 1.0.1 users should upgrade to the 2 more fixes available
High	OpenSSL-openssl-1.0.1				CVE-2016-2179	16-09-2016	12-07-2018	The vendor has issued a source code fix, avail 1 more fix available
High	OpenSSL-openssl-1.0.1				CVE-2016-2181	16-09-2016	20-04-2018	The vendor has issued a source code fix, avai
High	OpenSSL-openssl-1.0.1				CVE-2016-2183	01-09-2016	24-10-2018	All OpenSSL users should upgrade to the lates
High	OpenSSL-openssl-1.0.1				CVE-2016-6302	16-09-2016	14-07-2018	The vendor has issued a fix (1.0.1u, 1.0.2i, 1.1.0
High	OpenSSL-openssl-1.0.1				CVE-2016-6304	26-09-2016	20-04-2018	All OpenSSL users should upgrade to the lates 2 more fixes available

---

Container Policies

Enforce policies based on the deployment lifecycle: Kubernetes is the final stage of the deployment, so we would want to be very restrictive in terms of enforcing policies. Once a policy is defined, you will get an automated alert if new vulnerabilities are detected in the existing cluster, and the resources will be automatically rejected when attempting deployment.

Add Policy

Name

Reject High Security Vulnerabilities

Product Deployment Storage

Kubernetes

Match

By Security Vulnerability Severity   ▼

Vulnerability Severity

◉ High
○ Medium
○ Low

The policy will perform the action on libraries that have at least one security vulnerability with the selected severity.

WhiteSource