

# Mend.io for Containers

## Scalable Security for Cloud-Native Applications

### The Challenge

Cloud-native application development introduces new potential for application risk from multiple sources. Even organizations that have implemented strong security controls and risk management practices in the “left” side of the software development life cycle can have those efforts thwarted if new risks are introduced during the process of containerization.

Organizations need visibility over their container images at scale, including the ability to understand where risks come from and which containers should be prioritized for remediation in their source repositories. Because remediating during or after deployment is significantly more costly than remedying defects earlier in the SDLC, it's important for container alerts to focus exclusively on real risks, without false positives.

### The Mend.io Solution

Mend.io includes a full set of container image scanning features in Mend SCA to help reduce the risks associated with cloud-native application development. Mend for Containers scans container images and container image registries for potential risks including:

- Vulnerable open source components
- License risks in components (including operating system packages)
- Exposed secrets (encryption keys, passwords)

Risks to container images can be prioritized according to their EPSS score, and organizations can create and automatically enforce policies for approval and remediation of containers with detected risks.

When a risk is identified in container images, Mend SCA can trace the risk back to the source code repository where it originated, allowing it to be remediated quickly so a new version can be built and deployed.

### Why Mend.io?

**Mend.io offers a comprehensive code-to-cloud solution to minimize application development risk. Using Mend for Containers, you can:**

#### See Into Your Containers

Understand the components and supply chain that make up your containers for full visibility over your complete risk picture – from vulnerabilities and secrets to unwanted license types.

#### Screen Out False Positives

With runtime monitoring of container images in Kubernetes clusters, organizations can identify which risks are exploitable and require urgent remediation – and which can be safely ignored.

#### Close the Remediation Loop

Instantly trace the source of your container risks to its original repository, so you can track down vulnerabilities and license issues and remediate them fast.

#### Scan at Scale

Scan your container image registries to get a holistic view of your container risk and prioritize which containers to patch first.

#### Enforce Container Risk Policies

Automatically enforce approval and remediation policies to ensure that containers that violate policies are not able to deploy without requesting and obtaining approval for a policy exception.

## Mend SCA Protects Applications From Code to Cloud

Mend supports teams in every phase of the software development life cycle. Mend integrates with IDEs, repositories, registries, and CI/CD pipelines, and now scans container images and container image registries – providing automated risk remediation and policy enforcement that works while you code, build, deploy, and improve your applications.



## Protect Your Cloud-Native Applications with Mend.io

The full set of Mend for Containers features is included with every Mend SCA license. There's no need to buy an extra product to stay protected through the entire SDLC – through cloud deployment and beyond.

Ready to take the next step to protecting your applications from open source risk?  
We'd love to learn more about your security needs and what you're looking for.  
Contact us today at [sales@mend.io](mailto:sales@mend.io) for more information or to set up a product tour.



## About mend.io

Mend.io, formerly known as WhiteSource, effortlessly secures what developers create. Mend.io uniquely removes the burden of application security, allowing development teams to deliver quality, secure code, faster. With a proven track record of successfully meeting complex and large-scale application security needs, the world's most demanding software developers rely on Mend.io. The company has more than 1,000 customers, including 25 percent of the Fortune 100, and manages Renovate, [link here](#), the open- source automated dependency update project.

For more information, visit [www.mend.io](http://www.mend.io), the Mend.io blog, and Mend.io on LinkedIn and Twitter.