Mend
Container

Mend AppSec Platform: Mend Container

Development to Deployment Coverage for Cloud-Native Applications

The Challenge

Cloud-native development brings new potential risks to applications and an added layer of complexity to application security. The customary "shift left" approach finds vulnerabilities in code early during development, but misses those vulnerabilities that sneak in later during the containerization process.

Containers put another level of abstraction between security teams and the code, increasing the difficulty of tracking down vulnerabilities, assessing risk levels,enforcing policies. Additional problems unique to containers also emerge, such as poorly stored secrets that can be found by bad actors, potentially handing them the keys to the kingdom.

As with any modern application, scanning containers can result in a large volume of alerts, many of which are for vulnerabilities that are unreachable at runtime. A typical SCA scan can only give so much insight.

The Solution

At Mend.io, we think that managing risks to your containers requires a holistic approach to effectively leverage your container security solution. Part of the Mend AppSec Platform, Mend Container uses state-of-the-art reachability analysis in your container runtime environment to provide security risk detection and mitigation unique to cloud-native applications.

Mend Container operates by seamlessly integrating with your container runtime environment, performing in-depth reachability analysis to pinpoint potential vulnerabilities and attack paths that are specific to the dynamic nature of cloud-native applications. This proactive approach within complex containerized environments, empowers you to make informed decisions and take decisive action, ensuring your applications remain resilient against potential threats.

Why the Mend AppSec Platform?

Gain a clear view across the SDLC

A comprehensive, dedicated solution for containers, Mend SCA and Mend Container together cover single images to entire registries from development to deployment.

Get runtime insights early

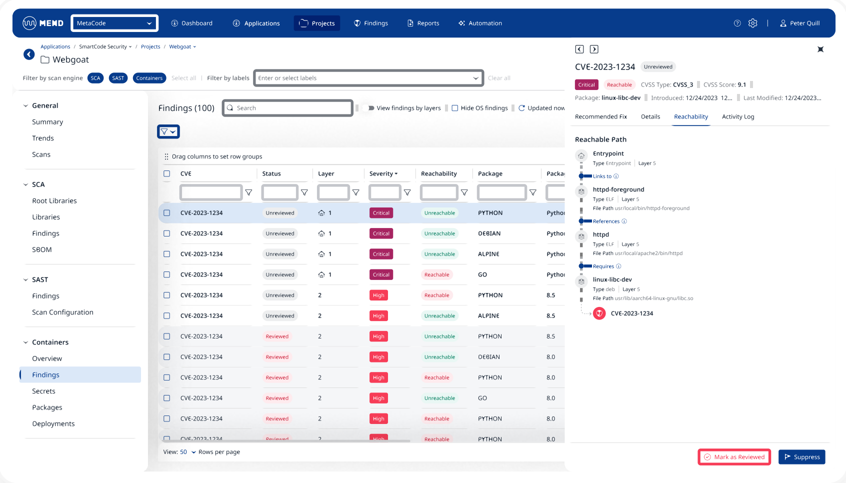
With Mend Container's container-level reachability, you can safely deprioritize vulnerabilities that are unreachable to your containers.

Quickly know what matters

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.

Keep your secrets safe

Find unprotected sensitive information such as API keys and passwords before malicious actors do.



Findings (100)

CVE	Status	Layer	Severity	Reachability	Package	Packa
CVE-2023-1234	Unreviewed	1	Critical	Unreachable	PYTHON	Python
CVE-2023-1234	Unreviewed	1	Critical	Unreachable	DEBIAN	Python
CVE-2023-1234	Unreviewed	1	Critical	Unreachable	ALPINE	Python
CVE-2023-1234	Unreviewed	1	Critical	Reachable	GO	Python
CVE-2023-1234	Unreviewed	2	High	Reachable	PYTHON	8.5
CVE-2023-1234	Unreviewed	2	High	Unreachable	ALPINE	8.5
CVE-2023-1234	Reviewed	2	High	Unreachable	PYTHON	8.5
CVE-2023-1234	Reviewed	2	High	Unreachable	DEBIAN	8.0
CVE-2023-1234	Reviewed	2	High	Reachable	PYTHON	8.0
CVE-2023-1234	Reviewed	2	High	Unreachable	GO	8.0
CVE-2023-1234	Reviewed	2	High	Reachable	PYTHON	8.0
CVE-2023-1234	Reviewed	2	High	Reachable	PYTHON	8.0

View: 50 Rows per page

CVE-2023-1234 Unreviewed

Critical Reachable CVSS Type: **CVSS_3** CVSS Score: **9.1**

Package: **linux-libc-dev** Introduced: 12/24/2023 12... Last Modified: 12/24/2023...

Reachable Path

Entrypoint
Type Entrypoint | Layer 5
Links to
httpd-foreground
Type ELF | Layer 5
File Path usr/local/bin/httpd-foreground
References
httpd
Type ELF | Layer 5
File Path usr/local/apache2/bin/httpd
Requires
linux-libc-dev
Type deb | Layer 5
File Path usr/lib/aarch64-linux-gnu/libc.so
CVE-2023-1234

Container Security Features & Capabilities You Get With The Mend AppSec Platform

Security teams choose Mend.io to add robust runtime protection.

Container reachability - The Mend AppSec Platform brings the application-level vulnerable method detection to runtime environments with Mend Container, identifying which vulnerable files and methods are being called at runtime without the need to install runtime agents.

Secrets detection - The Mend AppSec Platform uses Mend Container' secrets detection to identify credentials, passwords, keys, and certificates being exposed or handled inappropriately, putting your applications at risk.

Kubernetes cluster scanning - Effortlessly scan all of your running container images within your Kubernetes clusters, letting you easily find and label containers that are actually in use and deployed.

Development to deployment coverage - Comprehensive container security for your cloud-native applications, starting with static image scans in your pipeline using Mend SCA, all the way to container behavior analysis for security risks in runtime with Mend Container.

About Mend.io

Trusted by the world's leading companies, including IBM, Google, and Capital One, Mend.io's enterprise suite of application security tools is designed to help you build and manage a mature, proactive AppSec program.

Mend understands the different AppSec requirements of developers and security teams. Unlike other AppSec solutions that force everyone to use a single tool, Mend helps them work in harmony by giving each team different, but complementary, tools—enabling them to stop chasing vulnerabilities and start proactively managing application risk.