Mend
Container

AI Native AppSec Platform: Mend Container

Comprehensive cloud native AI security coverage

The Challenge

Cloud native development brings new potential risks to applications, including those powered by AI, 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, and 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. Security teams need a container solution that keeps pace with the increased velocity of AI development.

The Solution

Part of Mend.io's AI Native AppSec Platform, Mend Container provides comprehensive visibility into risks across the entire software development lifecycle. With image vulnerability scanning, reachability analysis, secrets detection, K8s integration, and security for AI components used to build containers, developers can secure applications at AI speed.

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.

With Mend Container, You Gain…

Container reachability analysis

Accurately predict what vulnerable files and methods will be called at runtime, as you build applications with AI, without needing to install runtime agents.

Secrets detection

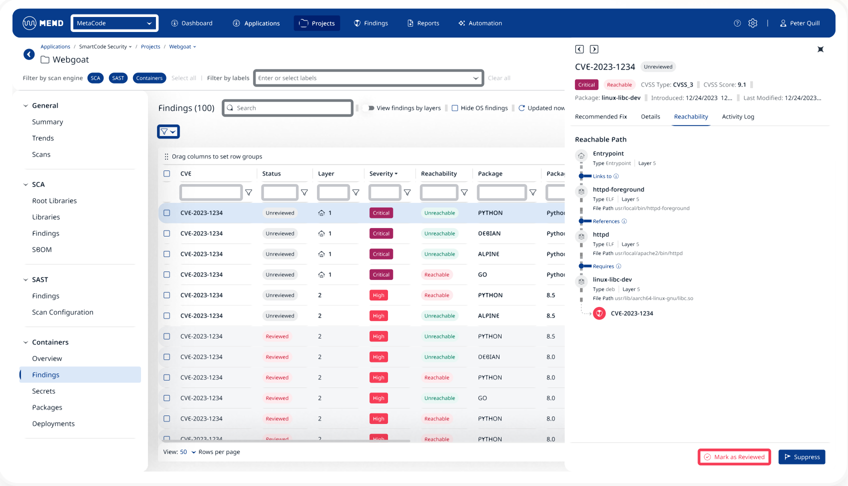
Find unprotected sensitive information such as API keys and passwords before malicious actors do.

Kubernetes cluster scanning

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 for AI pipelines

Find vulnerabilities in container images early in development, identify threats during runtime, and pinpoint the root location for rapid remediation.



Findings (100)

□	CVE	Status	Layer	Severity	Reachability	Package	Packa
□	CVE-2023-1234	Unreviewed	1	Critical	Unreachable	PYTHON	Pytho
□	CVE-2023-1234	Unreviewed	1	Critical	Unreachable	DEBIAN	Pytho
□	CVE-2023-1234	Unreviewed	1	Critical	Unreachable	ALPINE	Pytho
□	CVE-2023-1234	Unreviewed	1	Critical	Reachable	GO	Pytho
□	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

Mend.io

Why Mend.io’s AI Native AppSec Platform?

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

Gain a clear view across the SDLC - Comprehensive and dedicated container solution that provides visibility into risks across the entire software development lifecycle as you develop with AI.

Get runtime insights early - Bring application level vulnerability detection to runtime environments by accurately predicting what vulnerable files and methods will be called at runtime, in your AI powered applications, without needing to install runtime agents.

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 - keeping your AI powered applications secure from development to deployment.

Keep your secrets safe - Mend.io’s AI Native AppSec Platform uses Mend Container’ secrets detection to identify credentials, passwords, keys, and certificates being exposed or handled inappropriately, putting your applications at risk.