Leverage the combined strength of Mend.io and Sysdig for comprehensive container security

Traditional application security tools can leave many blind spots in containerized applications. Lacking visibility into what packages are in deployment leaves teams with no way to set preferred remediation priorities. Meanwhile, developers are inundated with alerts and end up spending precious time and resources fixing vulnerabilities that are not actually affecting their application – sabotaging their productivity.

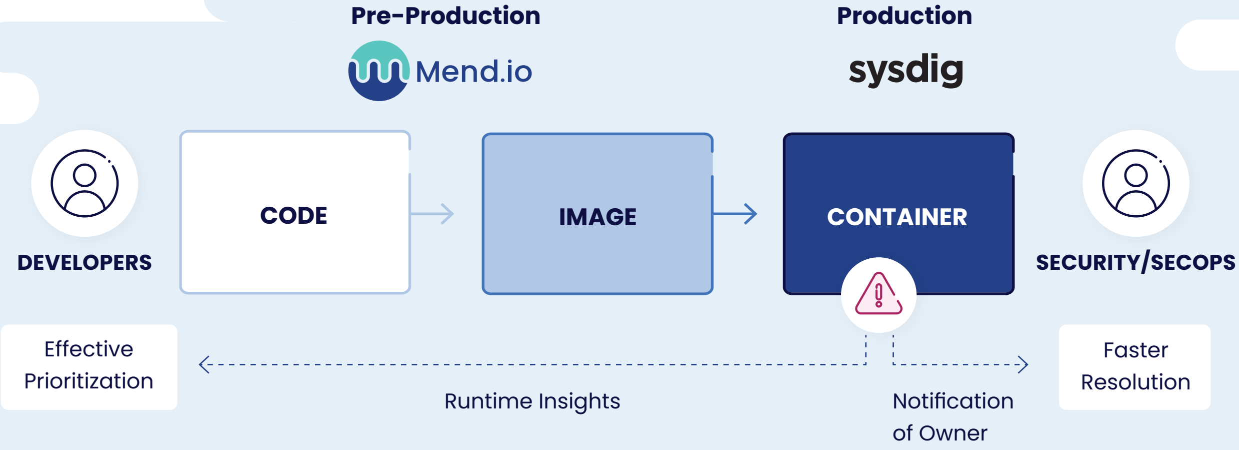
Now, customers running both Mend Container and Sysdig Secure can dramatically increase visibility and reduce noise across the SDLC and keep their applications secure from development to deployment.

Full Left to Right Coverage

The teams at Mend.io and Sysdig worked together to engineer a custom integration to best serve their joint customers. By combining “left side” and “right side” solutions, security teams and developers can spot real issues in production and swiftly find the culprit in the code.

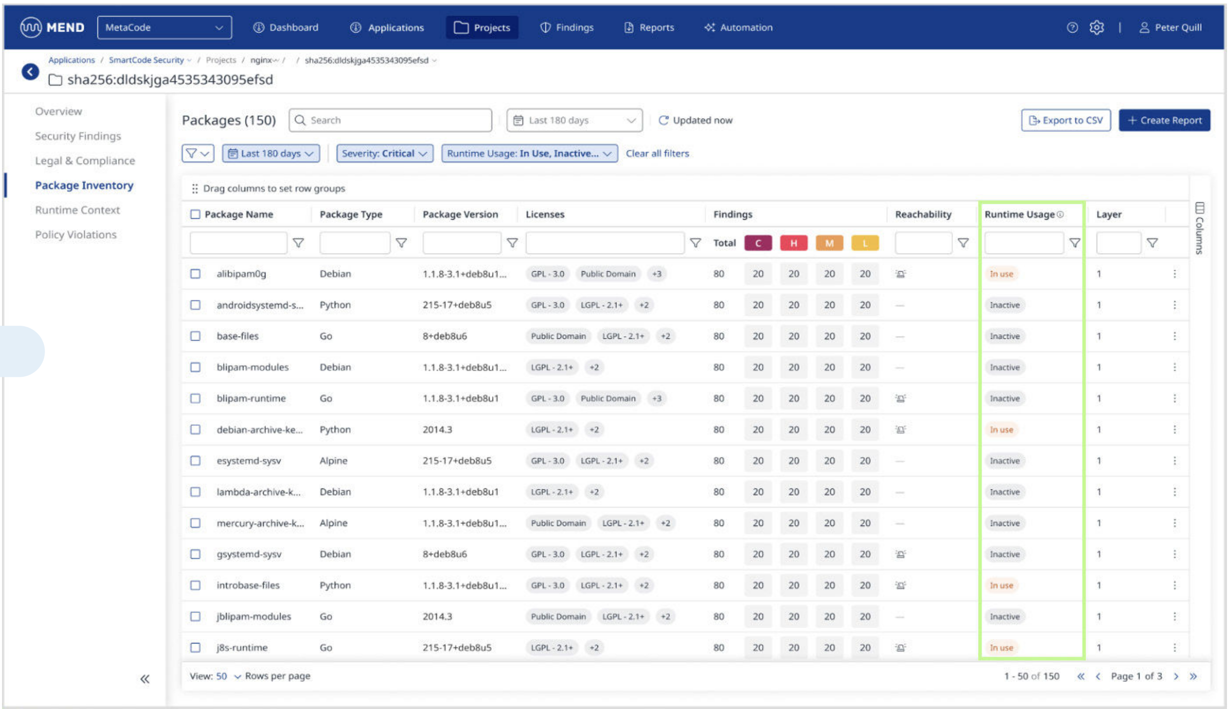
With a comprehensive approach to identifying and addressing vulnerabilities in your development and production environments, joint customers gain:

- **Runtime protection.** Optimize performance in real-time through continuous monitoring of your containerized applications, ensuring a responsive and secure environment.
- **95% reduction in vulnerability noise.** Swipe left on excess noise that’s slowing down and frustrating your developers. Provide them with insights into what packages are loading at runtime so they can effectively prioritize critical vulnerabilities to be fixed.
- **Development to deployment coverage.** Security teams can pinpoint the precise repository and application owner where the vulnerability was first introduced into development, accelerating remediation all the way from cloud to code.
- **Deployment priority control.** Take charge over application deployment priorities while increasing efficiency and allowing developers to confirm production deployment and set preferred remediation priorities.



Focus on What Matters

Life is short. Your release cycles are even shorter. The insights brought to you by Mend.io and Sysdig improve developer productivity by reducing alerts and allowing developers to put their time and attention on only the most crucial security concerns found in their containers.



Applications / SmartCode Security / Projects / nginx / / sha256:dldskjga4535343095efsd

sha256:dldskjga4535343095efsd

Packages (150)

Last 180 days

Filters: Last 180 days · Severity: **Critical** · Runtime Usage: **In Use, Inactive...** · Clear all filters

□ Package Name	Package Type	Package Version	Licenses	Findings					Reachability	Runtime Usage	Layer
				Total	C	H	M	L			
□ alibipam0g	Debian	1.1.8-3.1+deb8u1...	GPL - 3.0 Public Domain +3	80	20	20	20	20	🚨	In use	1
□ androidsystemd-s...	Python	215-17+deb8u5	GPL - 3.0 LGPL - 2.1+ +2	80	20	20	20	20	—	Inactive	1
□ base-files	Go	8+deb8u6	Public Domain LGPL - 2.1+ +2	80	20	20	20	20	—	Inactive	1
□ blipam-modules	Debian	1.1.8-3.1+deb8u1...	LGPL - 2.1+ +2	80	20	20	20	20	—	Inactive	1
□ blipam-runtime	Go	1.1.8-3.1+deb8u1	GPL - 3.0 Public Domain +3	80	20	20	20	20	🚨	Inactive	1
□ debian-archive-ke...	Python	2014.3	LGPL - 2.1+ +2	80	20	20	20	20	🚨	In use	1
□ esystemd-sysv	Alpine	215-17+deb8u5	GPL - 3.0 LGPL - 2.1+ +2	80	20	20	20	20	—	Inactive	1
□ lambda-archive-k...	Debian	1.1.8-3.1+deb8u1	LGPL - 2.1+ +2	80	20	20	20	20	—	Inactive	1
□ mercury-archive-k...	Alpine	1.1.8-3.1+deb8u1...	Public Domain LGPL - 2.1+ +2	80	20	20	20	20	—	Inactive	1
□ gsystemd-sysv	Debian	8+deb8u6	GPL - 3.0 LGPL - 2.1+ +2	80	20	20	20	20	🚨	Inactive	1
□ introbase-files	Python	1.1.8-3.1+deb8u1...	GPL - 3.0 LGPL - 2.1+ +2	80	20	20	20	20	🚨	In use	1
□ jblipam-modules	Go	2014.3	Public Domain LGPL - 2.1+ +2	80	20	20	20	20	—	Inactive	1
□ j8s-runtime	Go	215-17+deb8u5	LGPL - 2.1+ +2	80	20	20	20	20	🚨	In use	1

View: 50 Rows per page

1 - 50 of 150 « ‹ Page 1 of 3 › »

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.

Learn more at www.mend.io

About Sysdig

In the cloud, every second counts. Attacks move at warp speed, and security teams must protect the business without slowing it down. Sysdig stops cloud attacks in real time, instantly detecting changes in risk with runtime insights and open source Falco. Sysdig correlates signals across cloud workloads, identities, and services to uncover hidden attack paths and prioritize real risk. From prevention to defense, Sysdig helps enterprises focus on what matters: innovation.

Sysdig. Secure Every Second.

Mend.io