mend.io

Mend SCA or Mend Supply Chain Defender?

Protecting the Software Supply Chain with Mend.io

The Challenge

Supply chain attacks are on the rise, spiking an average of 740 percent year on year from 2019 to 2022. One of the most challenging sources of supply chain risk: malicious open source packages, which plant unwanted code into your applications by camouflaging themselves as the open source libraries your developers depend on. The number of these packages quadrupled from 2021 to 2022.

Detecting these impostors – and replacing them with the non-compromised library version your developers wanted – is key to protecting your software supply chain. Left unchecked, malicious packages can deploy ransomware, delete files, or quietly export your sensitive information to threat actors. There's only one right number of malicious packages for your application code: zero.

The Solution

Mend.io offers two ways to identify and block malicious packages before they are downloaded by developers and enter your code base. One is our free developer tool, Mend Supply Chain Defender. The other is Mend SCA with 360° Malicious Package Protection. Both are capable of blocking malicious open source packages. So what's the difference?

Head To Head: Mend SCA vs. Mend Supply Chain Defender

	Mend SCA with 360° Malicious Package Protection	**Mend Supply Chain Defender**
Industry-leading accuracy in detecting malicious packages	**Yes**	**Yes**
Malicious package blocking	**Yes**	**Yes**
Malicious package detection in existing code	**Yes**	**No**
Smart Merge Control for smart, non-breaking automated updates	**Yes**	**No**
Deploys in	Repository, Pipeline, Artifact Registry	Package managers
Best for	Entire organizations	Individual developers
Automated vulnerability fixes	**Yes**	**No**
Automated secure dependency updates	**Yes**	**No**
Open source license risk detection	**Yes**	**No**
Due diligence reporting	**Yes**	**No**
SBOM creation	**Yes**	**No**
Cost	Paid per contributing developer	Free

The Quick Check For Individual Developers: Mend Supply Chain Defender

Mend Supply Chain Defender works as an add-on to popular package managers including npm and RubyGems. Individual developers install Supply Chain Defender in order to block malicious packages from being downloaded. With world-class researchers who are frequently the first discoverers of malicious packages – rather than just detecting packages other researchers have identified as malicious – Supply Chain Defender offers up-to-the-minute protection from this growing threat.

For individual developers, Mend Supply Chain Defender is a great way to protect themselves from downloading malicious packages that disguise themselves with typosquatting or dependency confusion techniques. However, it was not designed as a tool to deploy across an enterprise, with unified visibility: it is solely a tool to be applied by developers on their own.

The Enterprise-Ready Solution: Mend SCA with 360° Malicious Package Protection

For maximum protection from malicious packages, Mend SCA now comes standard with 360° Malicious Package Protection, offering both blocking of newly downloaded malicious packages and detection of existing malicious packages already in your software supply chain. With built-in SBOM generation capabilities, Mend SCA with 360° Malicious Package Protection gives you the ability to prove your supply chain is safe.

Designed to maximize security teams' visibility over open source risks with minimal risk to developers, Mend SCA also makes it possible to set policies for open source licensing and vulnerability risks, allowing security teams to enforce these policies at the development gates of their choosing (pull request, push, commit, build).

About Mend.io

Mend.io, formerly known as WhiteSource, has over a decade of experience helping global organizations build world-class AppSec programs that reduce risk and accelerate development—using tools built into the technologies that software and security teams already love. Our automated technology protects organizations from supply chain and malicious package attacks, vulnerabilities in open source and custom code, and open-source license risks. With a proven track record of successfully meeting complex and large-scale application security needs, Mend.io is the go-to technology for the world's most demanding development and security teams. The company has more than 1,000 customers, including 25 percent of the Fortune 100, and manages Renovate, the open source automated dependency update projectFor more information, visit www.mend.io, the Mend blog, and Mend on LinkedIn and Twitter.