MEND

# Supply Chain Defender

## The Challenge

Software supply chain attacks have become a major application security threat.

When malicious code is surreptitiously added to software libraries that are used by applications, the potential of damage is severe. Such attacks have the potential to compromise not only developer machines and accounts but also testing and production infrastructure.  According to research conducted in 2021, supply chain attacks are now the second most common source of breach..

Scanning for malicious packages after they are installed is too late — similar to scanning for a virus which is already on your computer. In order to address the rising threat of this type of attack, software development teams need AppSec tools that go beyond detection to include continuous prevention. But how can organizations ensure they are protected from supply chain security threats without interrupting developers' work and delaying delivery?

## The Solution

Mend Supply Chain Defender is a software supply chain security solution that prevents the installation of malicious packages from the earliest stages of the development cycle.

Since its public launch in early 2020, Mend Supply Chain Defender has been responsible for identifying 100% of the known malicious packages posted to RubyGems, and over 4500 malicious packages on the npm registry since late 2021. Mend Supply Chain Defender continuously scans both registries to detect uploads of new malicious packages within minutes. Once a package has been marked malicious, Mend Supply Chain Defender will alert and block any attempted downloads of the package.

Mend Supply Chain Defender can be deployed by individual developers via a plugin to their package managers. Alternatively, enterprises using JFrog Artifactory and Mend SCA Enterprise can activate Mend Supply Chain Defender in a centralized fashion to protect all projects linked to their JFrog Artifactory registries.

## Top Benefits

### 1 Detect and block malicious open source software

**Mend Supply Chain Defender** detects suspicious packages in real-time and blocks the installation of malicious packages. It assesses open source component permissions and alerts on suspicious ones, and also blocks packages that were taken over, tampered with, or that include malware.

### 2 Shift left supply chain security to free up developer time

Thanks to innovative classification rules for suspicious components, Mend Supply Chain Defender is the ultimate shift left tool. It blocks suspicious packages before they can reach a developer's machine to enable developers to work uninterrupted with code they can trust.

### 3 Supported by Mend

**Mend Supply Chain Defender** is part of Mend's Application Security Platform that secures open source software, custom code, and infrastructure as code.

# MENDSupply Chain Defender

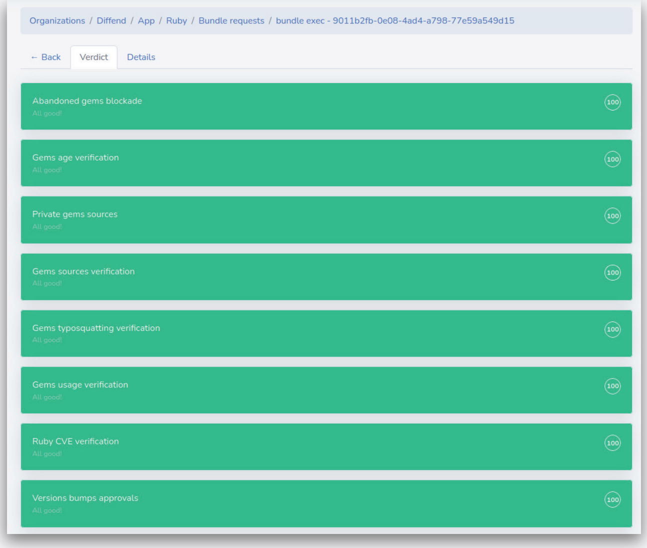
## Product Specifications

| | |
|---|---|
| Languages (and supported package managers) | Ruby 2.5+ (Bundler 2.1.x, 2.2.x)<br>Javascript (Yarn 2.4.1, npm, pnpm) |
| Reporting | UI notifications, Slack notifications |

## MAIN SCREENS:

### “Allow” verdict issued when Mend Supply Chain Defender believes dependencies to be safe.

When a package’s install/update command is executed, the Mend Supply Chain Defender package manager plugin aggregates all of the details about packages and sends them to Mend’s threat research center. If the packages are safe, an allow verdict is returned with the result details.


Organizations / Diffend / App / Ruby / Bundle requests / bundle exec - 9011b2fb-0e08-4ad4-a798-77e59a549d15
← Back
Verdict
Details

Abandoned gems blockade
All good! 100

Gems age verification
All good! 100

Private gems sources
All good! 100

Gems sources verification
All good! 100

Gems typosquatting verification
All good! 100

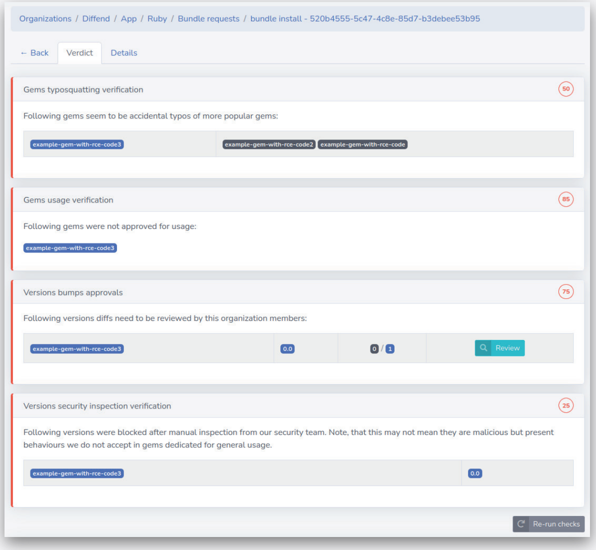
Gems usage verification
All good! 100

Ruby CVE verification
All good! 100

Versions bumps approvals
All good! 100

### “Deny” verdict issued when Mend Supply Chain Defender believes dependencies to be malicious.

When a negative (deny) verdict is issued, all the details about it are available via the Mend Supply Chain Defender web UI.


Organizations / Diffend / App / Ruby / Bundle requests / bundle install - 520b4555-5c47-4c8e-85d7-b3debee53b95
← Back
Verdict
Details
Review
Re-run checks

Gems typosquatting verification 50

Following gems seem to be accidental typos of more popular gems:

example-gem-with-rce-code3 | example-gem-with-rce-code2 example-gem-with-rce-code

Gems usage verification 85

Following gems were not approved for usage:

example-gem-with-rce-code3

Versions bumps approvals 75

Following versions diffs need to be reviewed by this organization members:

example-gem-with-rce-code3 | 0.0 | 0 / 1

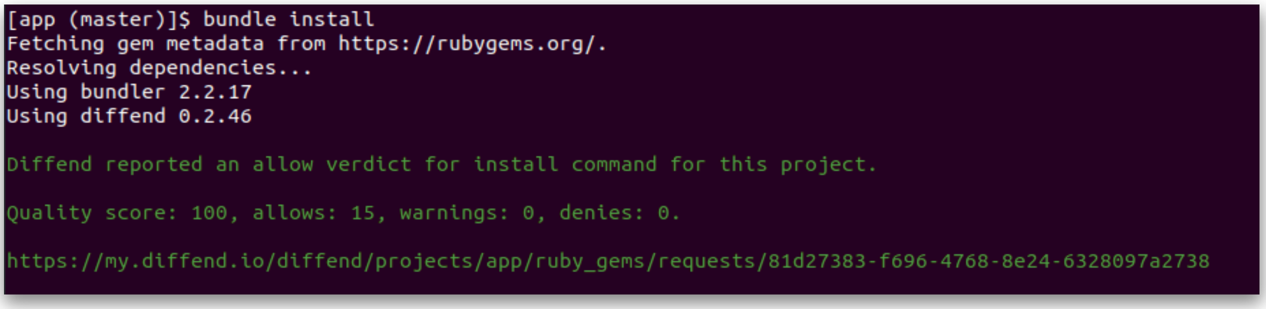
Versions security inspection verification 25

Following versions were blocked after manual inspection from our security team. Note, that this may not mean they are malicious but present behaviours we do not accept in gems dedicated for general usage.

example-gem-with-rce-code3 | 0.0

## Verdict results are visible from the CLI when running dependencies install command.

The moment Mend Supply Chain Defender issues the verdict, basic information is visible in the user shell.



```
[app (master)]$ bundle install
Fetching gem metadata from https://rubygems.org/.
Resolving dependencies...
Using bundler 2.2.17
Using diffend 0.2.46

Diffend reported an allow verdict for install command for this project.

Quality score: 100, allows: 15, warnings: 0, denies: 0.

https://my.diffend.io/diffend/projects/app/ruby_gems/requests/81d27383-f696-4768-8e24-6328097a2738
```