WhiteSource

WHITESOURCE DIFFEND

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 for damage is severe — ranging from impacting application traffic to exposing sensitive systems and data.

Scanning for malicious content after a package has been installed is too late. 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:

WhiteSource Diffend is a comprehensive supply chain security solution designed for behind-the-scenes exception-based alerting that doesn't interfere with developers' work.

It prevents any installations of malicious packages or malicious updates of existing packages from the earliest stages of the development cycle.

Since its public launch in early 2020, WhiteSource Diffend has detected over 350 known malicious packages on the Rubygems registry, and over 1400 malicious packages on NPM since late 2021. As such, WhiteSource Diffend has been directly responsible for the majority of such packages being "yanked", which in turn protects the entire community.

Top Benefits

WhiteSource Diffend manages the greatest risks associated with open source third-party dependencies.

1. Detect and block malicious open source software
WhiteSource Diffend both 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.

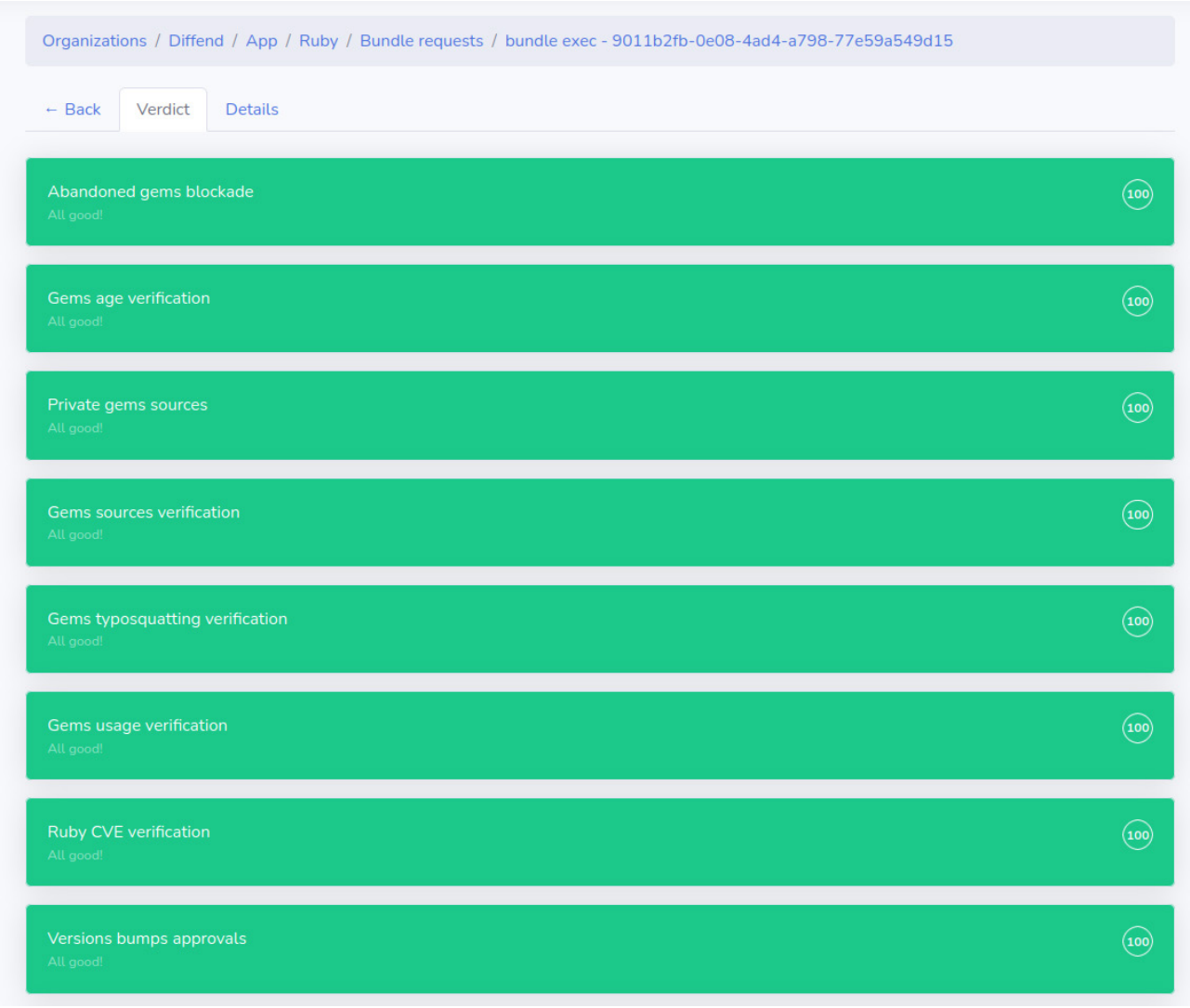
2. Shift left supply chain security to free up developer time
Thanks to innovative classification rules for suspicious components, WhiteSource Diffend is the ultimate shift left tool. It blocks suspicious packages before they can reach a developer's machine to enable developers to work uninterrupted with code they can trust.

3. Gain complete visibility over open source security and compliance
Integrated into the WhiteSource platform, WhiteSource Diffend helps organizations manage open source security and compliance throughout the development lifecycle, including analysis of open source licensing and other metadata.

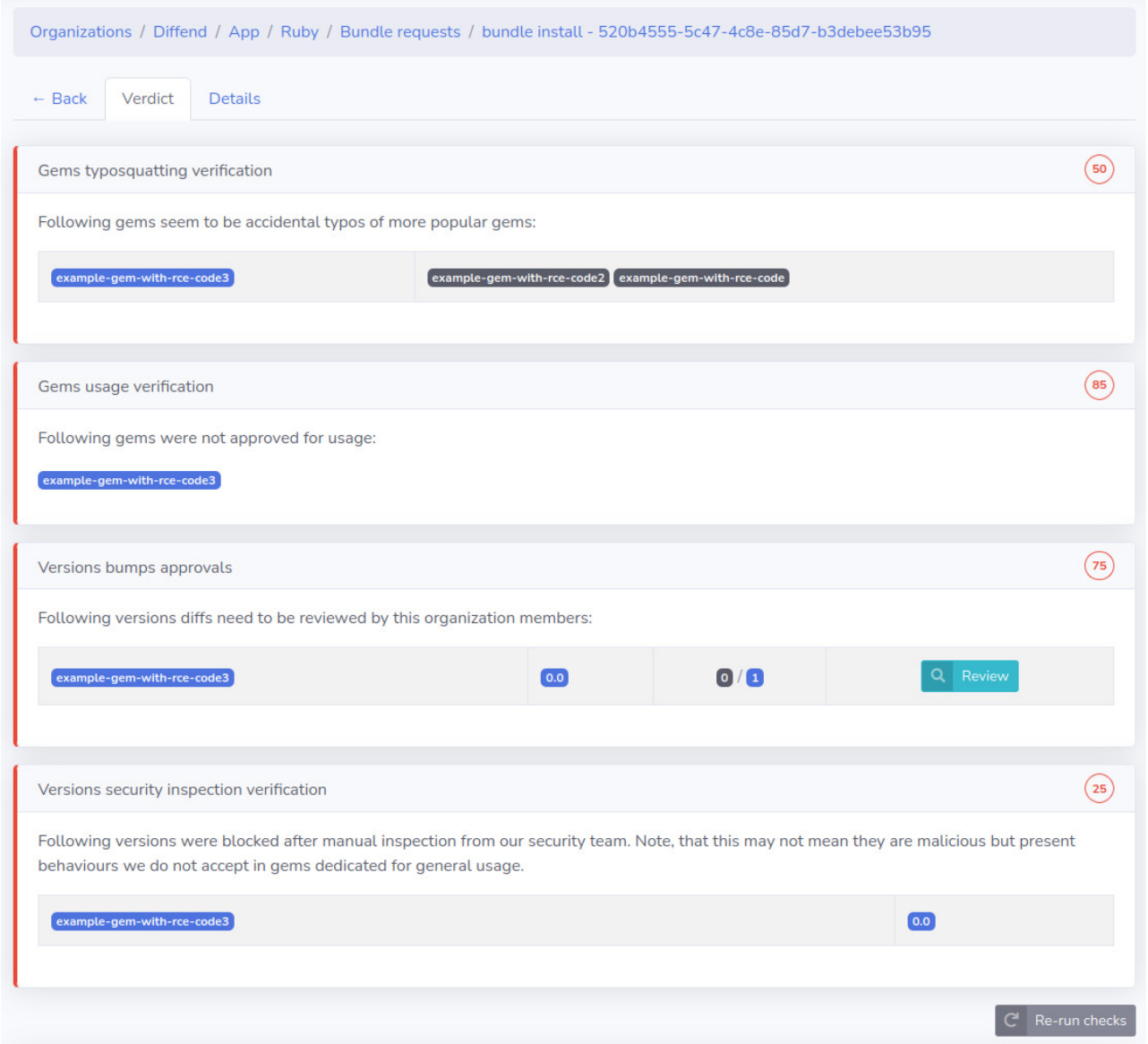
Languages	Ruby, Javascript
Package managers	RubyGems, Yarn 2 (beta)
Supported versions	Ruby: Ruby 2.5+ Node: 6.x + Bundler: 2.1.x, 2.2.x Yarn 2.4.1
Reporting	UI notifications, Slack notifications

MAIN SCREENS:

1. "Allow" verdict issued when WhiteSource Diffend believes dependencies to be safe.
When a package's install/update command is executed, the WhiteSource Diffend package manager plugin aggregates all of the details about packages and sends them to WhiteSource Diffend. It then receives an allow verdict -- available via the Web UI, with the result details.



2. "Deny" verdict issued when WhiteSource Diffend believes dependencies to be malicious.
When a negative (deny) verdict is issued, all the details about it are available via the Diffend web UI.



3. "Allow" verdict results are visible from the CLI when running dependencies install command.
The moment Diffend 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
```