ENJOYING OPEN SOURCE WITHOUT COMPROMISING BUSINESS

Rami Sass
CEO, WhiteSource Software
rami@whitesourcesoftware.com

Background

- I am a software engineer, not a legal expert
- My own experience with the dark side of open source
  - Managed R&D in an company during M&A in 2008
  - In the DD, we reported 30 libraries and licenses
  - We ended up with 250! (dependencies anyone?)
  - We were lucky! - no major "hidden surprises"
- What could we have (practically) done better?
- We started WhiteSource…

Open Source is Great, But…

- Open source substantially boosts developers productivity
  - 85% of new software projects, according to Gartner*
  - 80% of code in commercial products is actually OSS
- But, to enjoy the full value of open source, you must properly manage its use

* Source: Gartner User Survey Analysis: Open-Source Software, Worldwide

rami@whitesourcesoftware.com

Three Main Areas To Manage

Security and Quality Issues

License Risks and Compliance

Ineffective Management and Unnecessary Burden

rami@whitesourcesoftware.com

Security and Quality

- Most companies continue to ship products with open source that contains vulnerabilities, even long after these were fixed
  - 85% of software projects contain outdated open source *
- Like any other software, open source is likely to contain security vulnerabilities and other bugs
  - Rate of defects is 1 per 1,000 lines of code **
  - 70% of software applications contain security issues ***
- Open source communities are often quick to fix
- But OSS users are slow to update
- Why? Its difficult and out of scope for developers to be in the know

Vulnerabilities in open source you use are YOUR responsibility

rami@whitesourcesoftware.com

Sources: * WhiteSource, ** Coverity, *** Vercode

License Risks and Compliance

- Most companies lack a complete picture of all OSS libraries and licenses
  - In 60% of cases, gaps between reported and actual *
- License documentation is extremely tedious
  - Where done manually, lots of (hated) work, lots of errors
  - With scanners, lots of sifting through "false matches", delay release schedules
- One big reason is missed dependencies
  - 91% of open source libraries have dependencies *
  - 64% have a different license *
- Also, very few companies have license policies, and even fewer enforce policies in a consistent manner

Improper handling may result in legal, technical, and business risks

* Source: WhiteSource

rami@whitesourcesoftware.com

Ineffective Management and Unnecessary Burden

- Companies that do make an effort to manage their open source properly are wasting much effort
- 95% use manual processes
  - Licensing is the biggest challenge and one of most time consuming non-development task for developers *
  - And after expanding those efforts, lots of misses and errors lead to high risks
- Few use scanners
  - Expensive to buy; more expensive to operate – beyond the reach of any but the biggest companies
  - Issues are often discovered at worst time – M&A, OEM, Release – when most expensive to fix – rip and recode/replace

Developers shall develop. OSS management shall be automated.

* Source: JFrog

rami@whitesourcesoftware.com

Analysts

- *"As open source software becomes mainstream it requires the same level of security and reliability as proprietary software. Organizations must therefore implement processes and solutions to promptly identify and fix vulnerabilities in their open source software."*

  IDC Analyze the Future

  Dan Y., Research Director at IDC

  Emerging Technologies Group

- *"There is a clear disconnect between what is expected from development teams and what they can realistically do. They often lack the expertise and time to continually monitor open source libraries for security vulnerabilities and bugs."*

  stki.info THE KNOWLEDGE INTEGRATORS

  P. Cohen, EVP and Senior Analyst from STKI

rami@whitesourcesoftware.com

First Research – Dependencies and licenses

- Study of 500 software projects
- 37% of all open source components depend on other open source libraries. On average, each of these has 9 dependencies and 3 different open source licenses.
- 91% of open source projects contain indirect dependencies
- 65% of open source components were subject to additional licenses, due to dependencies.
- The most complex software project had 1917 open source dependencies.
- Most projects were subject to multiple licenses, with the maximum recorded at 26 licenses.
- 27% of all projects were subject to more than 10 different licenses
- 58% of all projects were subject to more than 5 different licenses.

rami@whitesourcesoftware.com

Second Research – Security

- study of 3,000 software projects with open source components found that 23% had security vulnerabilities.
- Meanwhile, only 1.3% of the open source libraries with vulnerabilities were updated with the latest version.
- Ninety-three percent of the vulnerabilities in infected open source libraries had either high or mid-range severity.
- 85% of project contain out-of-date libraries

rami@whitesourcesoftware.com

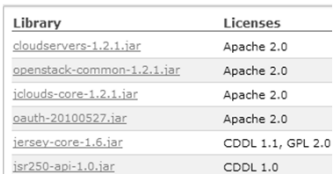
Bring Back the Full Value of Open Source

- Adopt a lifecycle approach
  - Deal with issues "at the door" and not post-hoc when difficult to discover and expensive to fix
  - Always updated inventory and risks dashboard at your fingertips
- Automate the discovery process
  - Don't depend on developers, and don't waste their time
- Enforce consistent license policy
  - Automate enforce when possible
  - Automate and document decision workflow when necessary
- Automate monitoring
  - Security issues and other bugs
  - New versions and fixes

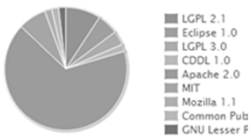
rami@whitesourcesoftware.com

WhiteSource

- Modern, cloud-based, SaaS service
  - Nothing to deploy and keep updating
  - No training needed
  - Not exposed to your proprietary code
- Integrates into your dev environment
  - Plugins to your build/CI server
  - Always current inventory and licenses
- Enforces license policy "at the door"
  - Detects new open source
  - Auto approve/reject
  - Approval workflow if necessary



Library	Licenses
cloudservers-1.2.1.jar	Apache 2.0
openstack-common-1.2.1.jar	Apache 2.0
jclouds-core-1.2.1.jar	Apache 2.0
oauth-20100527.jar	Apache 2.0
jersey-core-1.6.jar	CDDL 1.1, GPL 2.0
jsr250-api-1.0.jar	CDDL 1.0

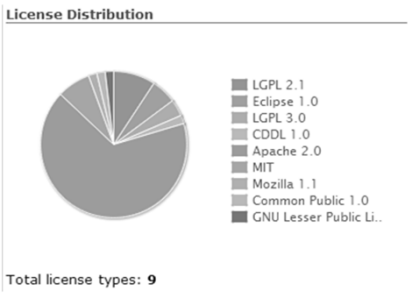


Policy name	Match	Action
Reject GPLs	By License Group	Reject
Reassign LGPL	By License Group	Reassign
Easy licenses	By License Group	Approve

rami@whitesourcesoftware.com

License Risks and Compliance

- Automatically document existing open source inventory
- Automatically identify all licenses, including dependencies
- Automate enforcement of organizational license policy
- Automate documentation during version release



Confidential

Security and Quality

- Proactive alerts on security vulnerabilities that affect you
- Proactive alerts on new releases of libraries you use
- Detect libraries that you no longer use

Confidential

Automatic. Easy. Agile.

- Integral part of your development lifecycle
  - Wide range of OOTB plugins to leading build tools
  - Send signatures of libraries (not the code!) to WhiteSource
  - Entire open source content is discovered and categorized
  - Open source policy can be enforced (including stop build)
- Take developers out of the loop
  - Saves time. Lets developer focus on their work.
  - Increase precision and timeliness. Reduce errors.

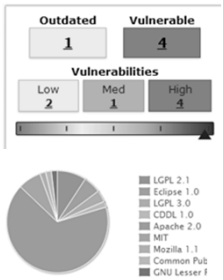
Confidential

DEMO

WhiteSource (2)

- Proactive alerts on security issues and fixes

- Dashboards and reports in a click
  - Ops: Inventory, Requests, Release automation
  - Compliance: licenses, risks
  - Quality and security: vulnerabilities, fixes



rami@whitesourcesoftware.com

WhiteSource

THANK YOU!

To manage OSS, adopt an approach that fits into and does not over-burden your development cycle

rami@whitesourcesoftware.com