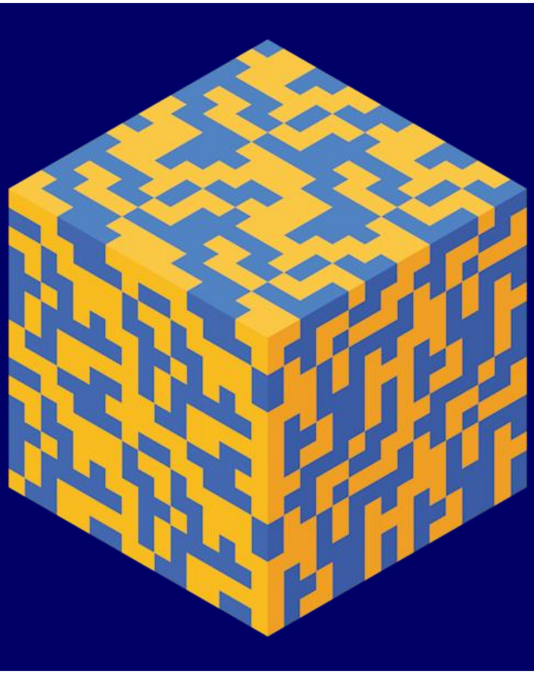


WhiteSource

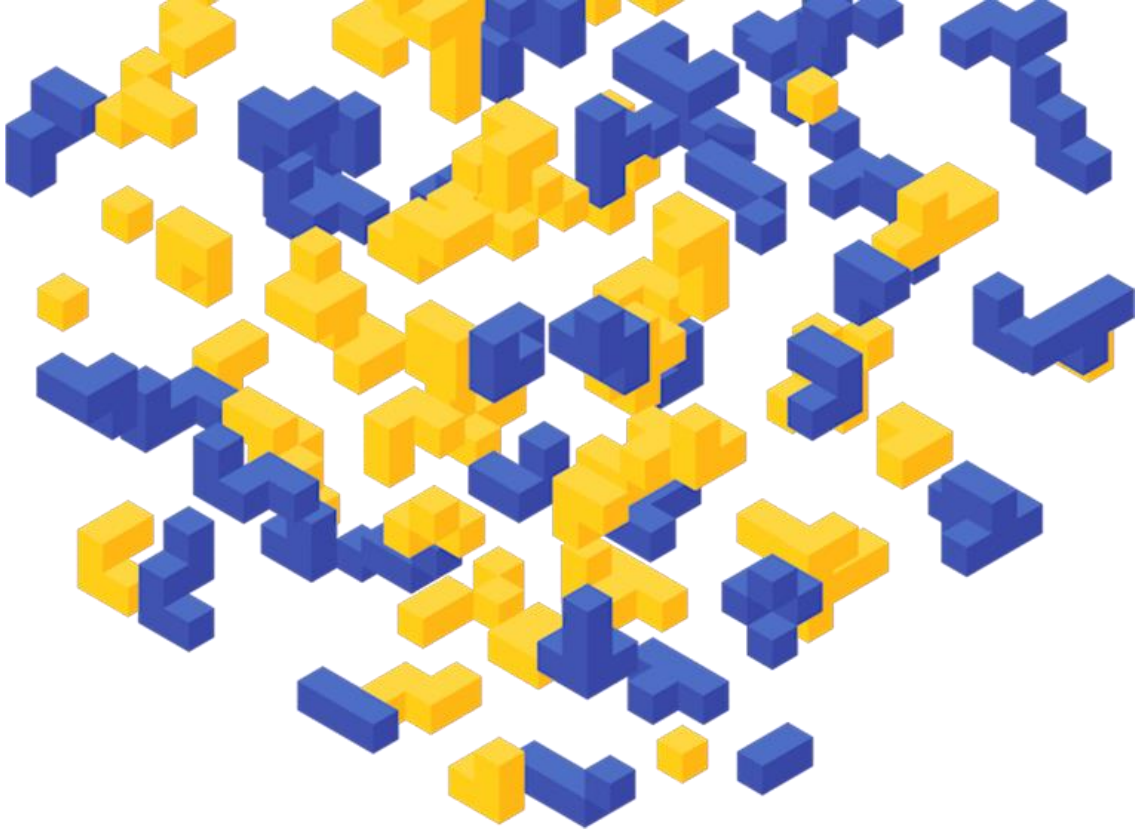
Managing the Risk and Growth of Using Open Source Software

Jason Hammond, CISSP
Director of Solutions Engineering – Channels

April 1, 2020

The Agenda

- The Growth of Open Source Software Use
- The Business Risks of Open Source Software Use
- Managing the Risks

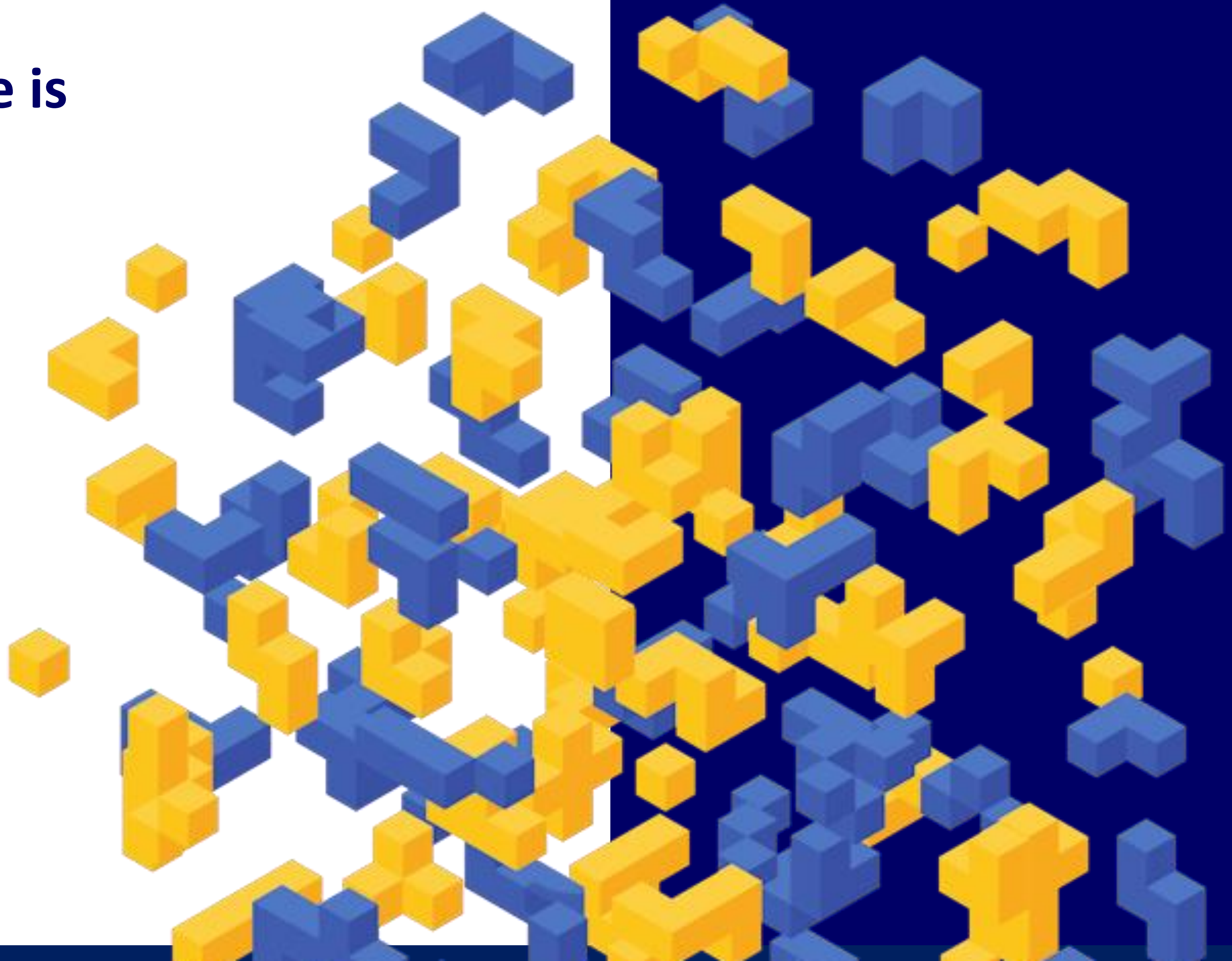


THE CHALLENGE

Open Source Software Use Is Growing

60-80%

of an average app's code base is comprised of open source



IT’S STILL UP TO YOU TO ENSURE YOUR PRODUCT

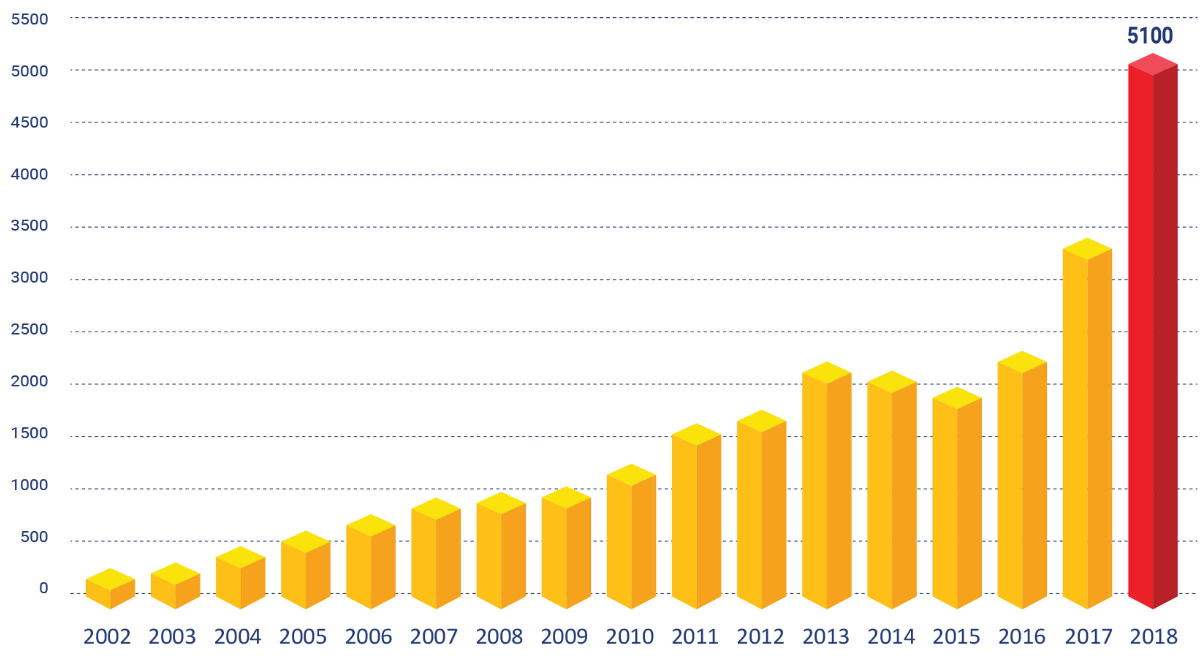
Doesn’t Contain Known Vulnerabilities

Compliant with Company’s Policies

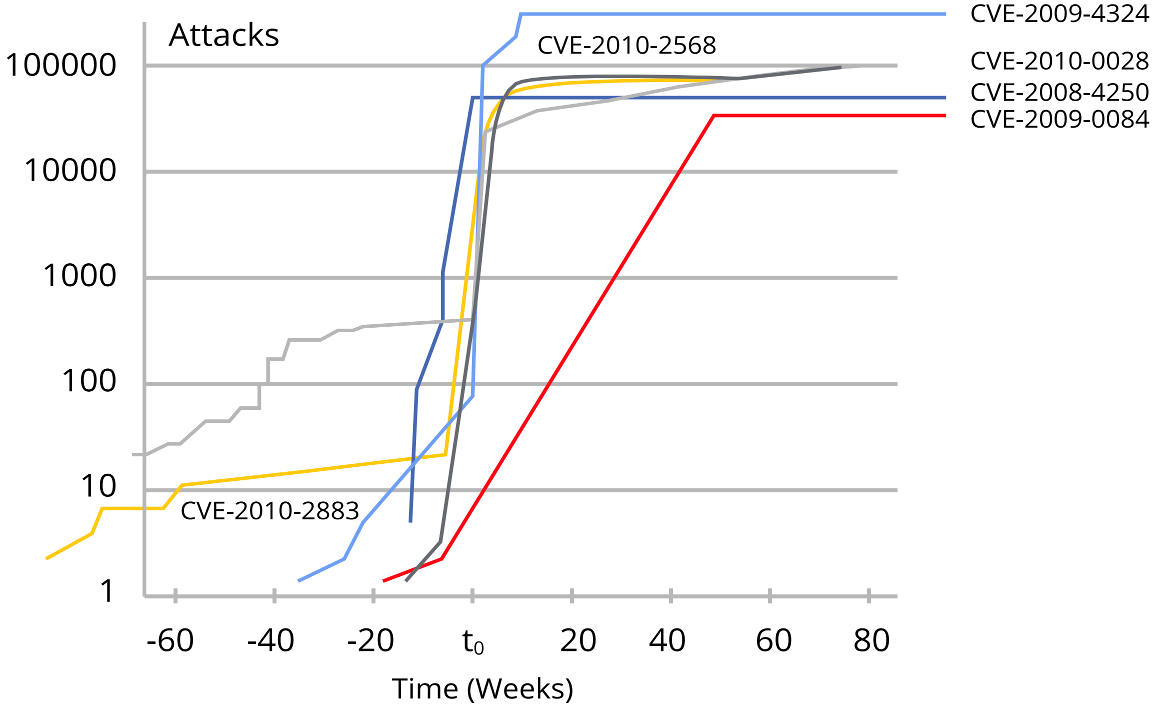
BUT IT’S NOT THAT EASY…

AND IT'S NOT GETTING ANY EASIER…

Reported Vulnerabilities Are Rising



Less Time To Fix

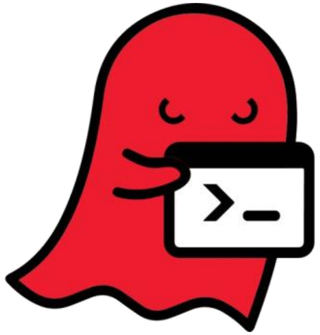


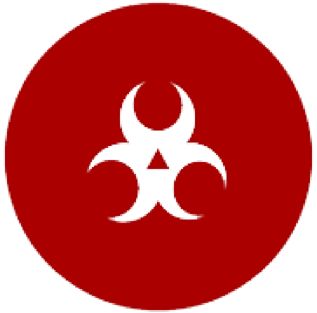
(a) Attacks exploiting zero-day vulnerabilities before and after the disclosure (time + t_0)

THE CHALLENGE

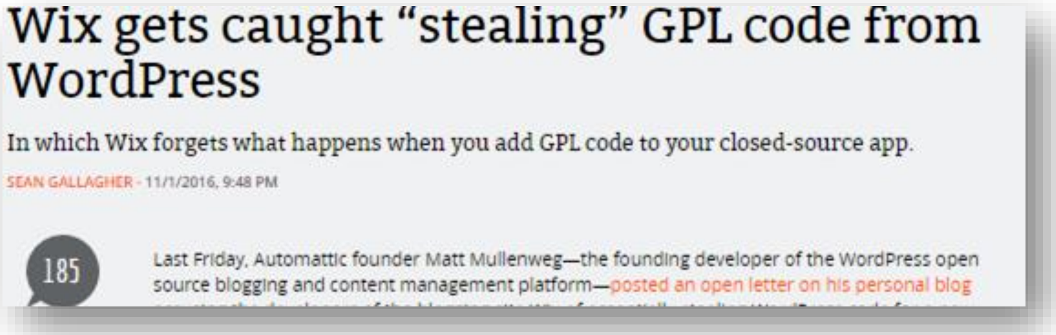
Open Source Software use can present risk to your business

Security Vulnerability Risk





License Risk



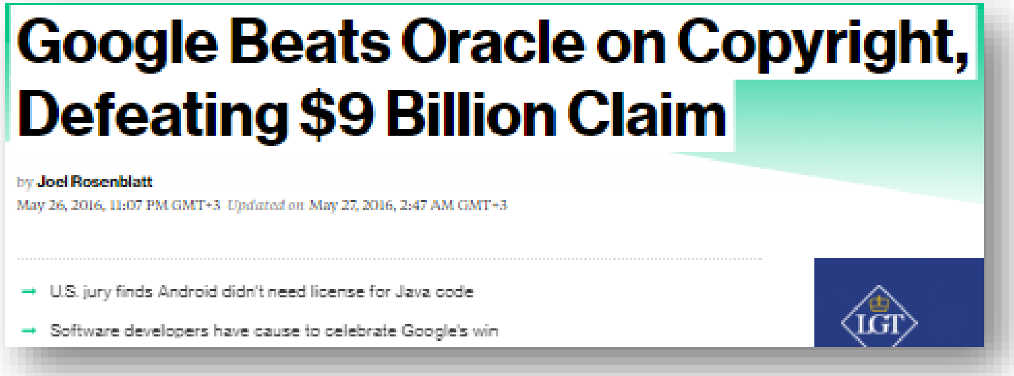
Wix gets caught “stealing” GPL code from WordPress

In which Wix forgets what happens when you add GPL code to your closed-source app.

SEAN GALLAGHER - 11/1/2016, 9:48 PM

185

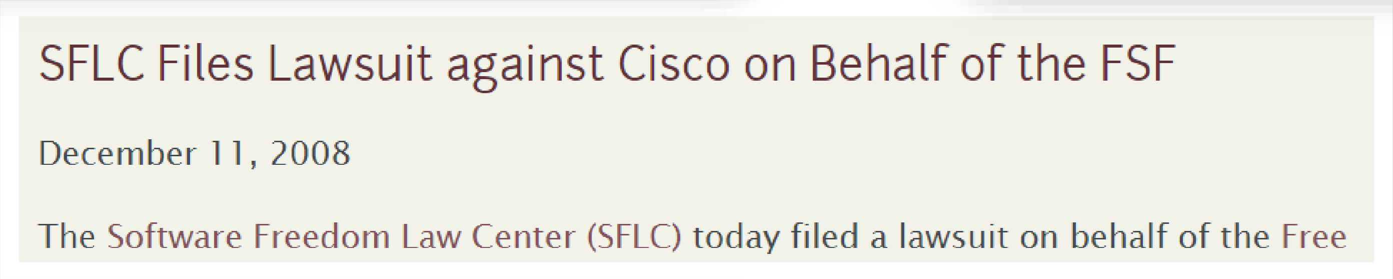
Last Friday, Automattic founder Matt Mullenweg—the founding developer of the WordPress open source blogging and content management platform—posted an open letter on his personal blog



Google Beats Oracle on Copyright, Defeating $9 Billion Claim

by Joel Rosenblatt
May 26, 2016, 11:07 PM GMT+3 *Updated on* May 27, 2016, 2:47 AM GMT+3

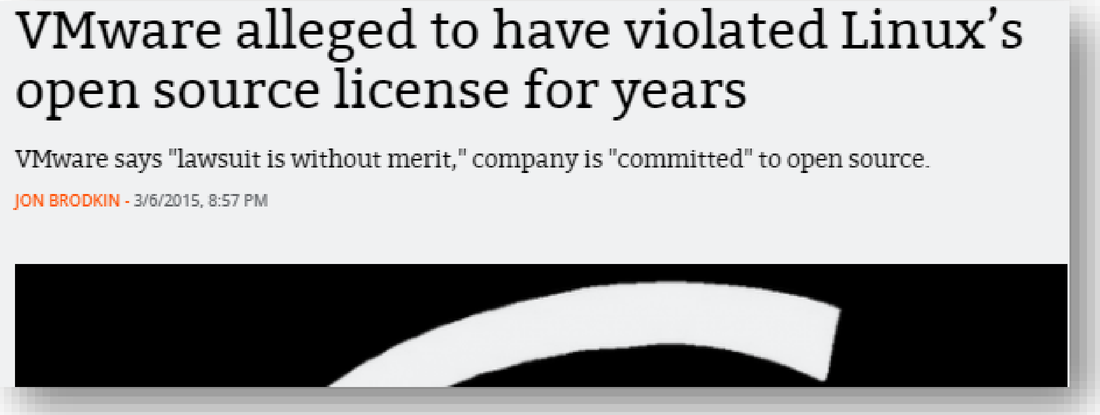
- U.S. jury finds Android didn't need license for Java code
- Software developers have cause to celebrate Google's win



SFLC Files Lawsuit against Cisco on Behalf of the FSF

December 11, 2008

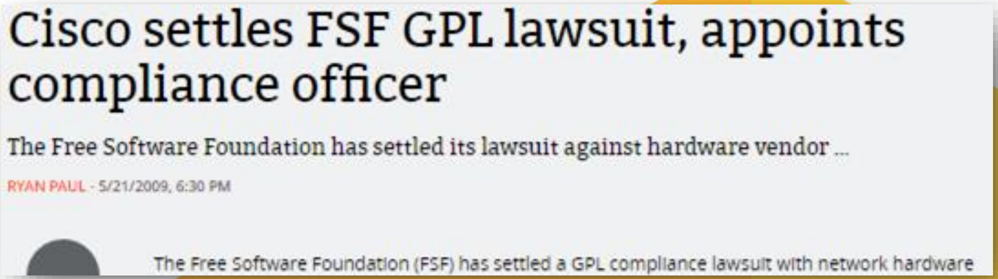
The Software Freedom Law Center (SFLC) today filed a lawsuit on behalf of the Free



VMware alleged to have violated Linux’s open source license for years

VMware says "lawsuit is without merit," company is "committed" to open source.

JON BRODKIN - 3/6/2015, 8:57 PM



Cisco settles FSF GPL lawsuit, appoints compliance officer

The Free Software Foundation has settled its lawsuit against hardware vendor ...

RYAN PAUL - 5/21/2009, 6:30 PM

The Free Software Foundation (FSF) has settled a GPL compliance lawsuit with network hardware

THE CHALLENGE

How to manage the risk of increased use of open source

SO HOW CAN YOU GET VISIBILITY AND CONTROL?

MANUAL

If you attempt to manually verify every component, you will slow down your developers.

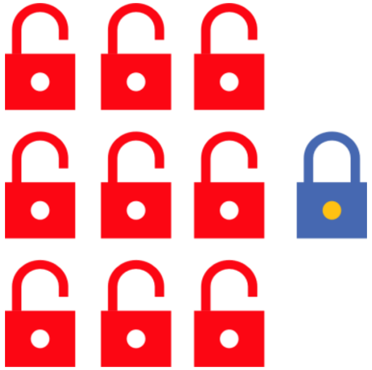
DO NOTHING

If you do nothing – you’re left exposed

AUTOMATION

LIFE WITHOUT OSS MANAGEMENT AUTOMATION

Over 75% were aware of only 50% of their open source inventory



90% of apps have at least **1 vulnerability**, over 45% have **5 or more**

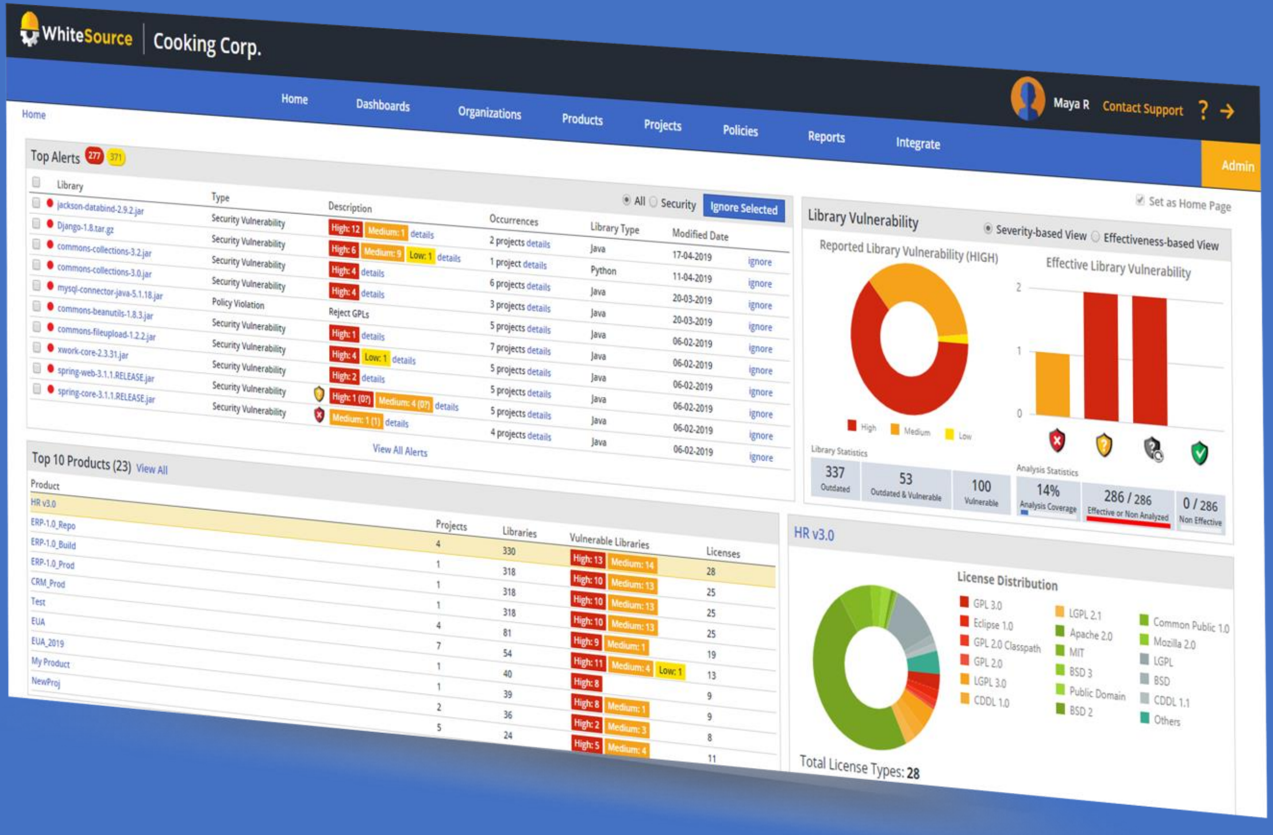
Broken dialog with Dev. Tough to explain where vulnerabilities are, and where is the risk

At least **1 license** that doesn’t meet company policy

* Based on first scan results for 250 applications and end of PoC questionnaire

AUTOMATED OPEN SOURCE SOFTWARE MANAGEMENT

Help You Develop Better Software, Faster by **Harnessing The Power of Open Source** Without Compromising on Security and Agility.



Top Alerts 277 371

● All ○ Security

□ Library	Type	Description	Occurrences	Library Type	Modified Date	
□ jackson-databind-2.9.2.jar	Security Vulnerability	High: 12 Medium: 1 details	2 projects details	Java	17-04-2019	ignore
□ Django-1.8.tar.gz	Security Vulnerability	High: 6 Medium: 9 Low: 1 details	1 project details	Python	11-04-2019	ignore
□ commons-collections-3.2.jar	Security Vulnerability	High: 4 details	6 projects details	Java	20-03-2019	ignore
□ commons-collections-3.0.jar	Security Vulnerability	High: 4 details	3 projects details	Java	20-03-2019	ignore
□ mysql-connector-java-5.1.18.jar	Policy Violation	Reject GPLs	5 projects details	Java	06-02-2019	ignore
□ commons-beanutils-1.8.3.jar	Security Vulnerability	High: 1 details	7 projects details	Java	06-02-2019	ignore
□ commons-fileupload-1.2.2.jar	Security Vulnerability	High: 4 Low: 1 details	5 projects details	Java	06-02-2019	ignore
□ xwork-core-2.3.31.jar	Security Vulnerability	High: 2 details	5 projects details	Java	06-02-2019	ignore
□ spring-web-3.1.1.RELEASE.jar	Security Vulnerability	High: 1 (0?) Medium: 4 (0?) details	5 projects details	Java	06-02-2019	ignore
□ spring-core-3.1.1.RELEASE.jar	Security Vulnerability	Medium: 1 (1) details	4 projects details	Java	06-02-2019	ignore

View All Alerts

Top 10 Products (23) View All

Product	Projects	Libraries	Vulnerable Libraries	Licenses
HR v3.0	4	330	High: 13 Medium: 14	28
ERP-1.0_Repo	1	318	High: 10 Medium: 13	25
ERP-1.0_Build	1	318	High: 10 Medium: 13	25
ERP-1.0_Prod	1	318	High: 10 Medium: 13	25
CRM_Prod	4	81	High: 9 Medium: 1	19
Test	7	54	High: 11 Medium: 4 Low: 1	13
EUA	1	40	High: 8	9
EUA_2019	1	39	High: 8 Medium: 1	9
My Product	2	36	High: 2 Medium: 3	8
NewProj	5	24	High: 5 Medium: 4	11

☑ Set as Home Page

Library Vulnerability

● Severity-based View ○ Effectiveness-based View

Reported Library Vulnerability (HIGH)

Effective Library Vulnerability

Library Statistics

337	53	100
Outdated	Outdated & Vulnerable	Vulnerable

Analysis Statistics

14%	286 / 286	0 / 286
Analysis Coverage	Effective or Non Analyzed	Non Effective

HR v3.0

License Distribution

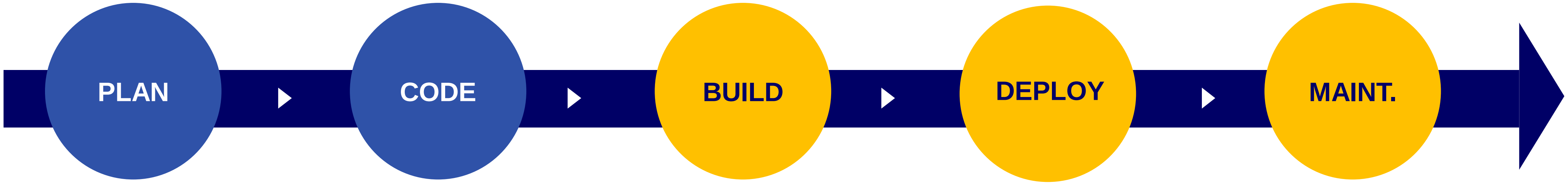
🟥 GPL 3.0	🟧 LGPL 2.1	🟩 Common Public 1.0
🟥 Eclipse 1.0	🟩 Apache 2.0	🟩 Mozilla 2.0
🟥 GPL 2.0 Classpath	🟩 MIT	▨ LGPL
🟥 GPL 2.0	🟩 BSD 3	▨ BSD
🟧 LGPL 3.0	🟩 Public Domain	▨ CDDL 1.1
🟧 CDDL 1.0	🟩 BSD 2	🟩 Others

Total License Types: 28

Automated Management Throughout The SDLC

For Developers

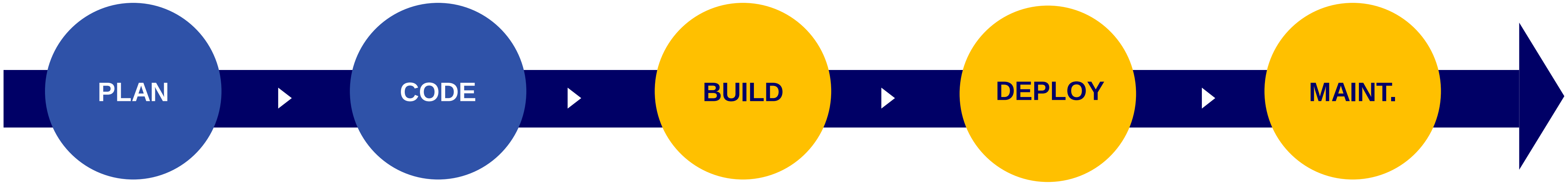
For Security & Compliance Professionals



Automated Management Throughout The SDLC

For Developers

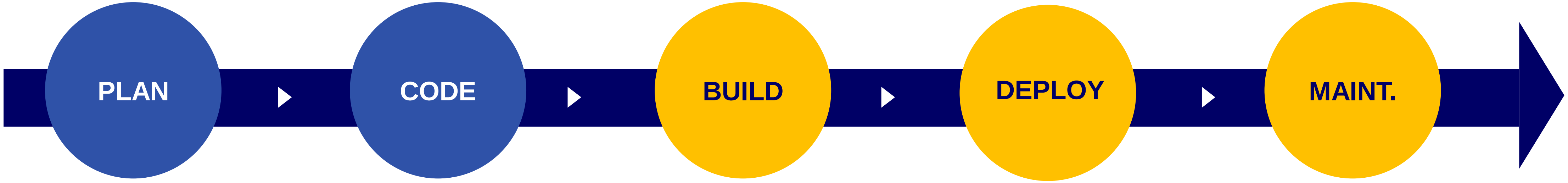
For Security & Compliance Professionals



Automated Management Throughout The SDLC

For Developers

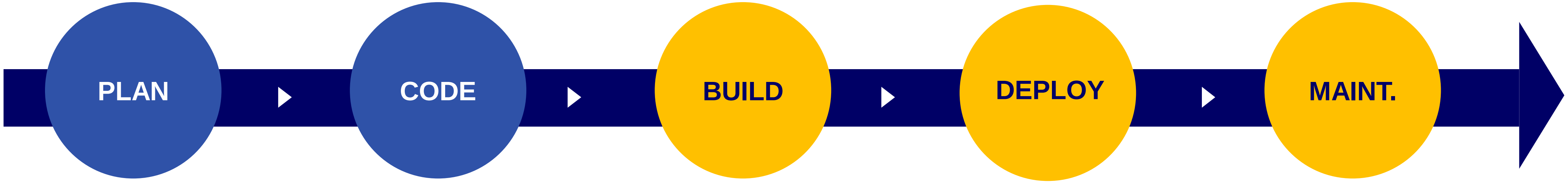
For Security & Compliance Professionals



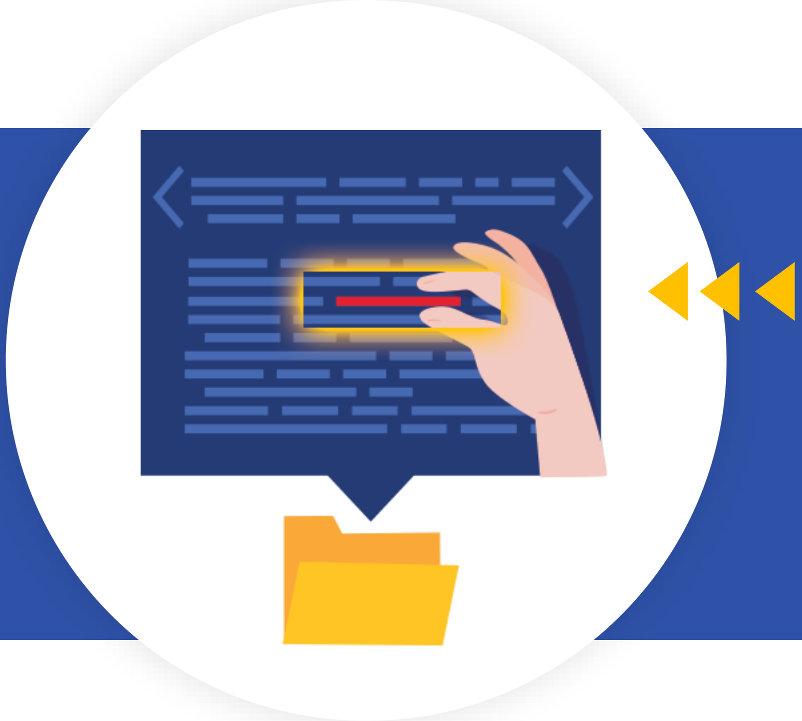
Automated Management Throughout The SDLC

For Developers

For Security & Compliance Professionals



WHY FIX ALL VULNERABILITIES
WHEN ONLY 15%-30% IMPACT YOUR PRODUCTS?



EFFECTIVE

VS

INEFFECTIVE

Open Source Libraries in Containers & Serverless

Open Source Management should be part of your Container Development Lifecycle

Development

Build

Container Registry

Deploy

Advanced integrations with all common container registries

AWS ECR

JFrog ARTIFACTORY

Automatic policy enforcement & continuous monitoring with Kubernetes integration

kubernetes

What to look for in an OSS Mgmt. Automation Solution

COMPLETENESS

Supporting over 200 programming languages. All environments. All groups, complete solution.

PRIORITIZATION

We help you focus on what matters with vulnerabilities prioritization and no false positives.

REMEDIATION

We not only alert, but also provide actionable, validated remediation tools to enable quick resolution.

THANK YOU

For more info please contact us: partners@whitesourcesoftware.com

WhiteSourceSoftware.com