2016 STATE OF THE SOFTWARE SUPPLY CHAIN

Sonatype

MAKING INVISIBLE **THINGS VISIBLE**

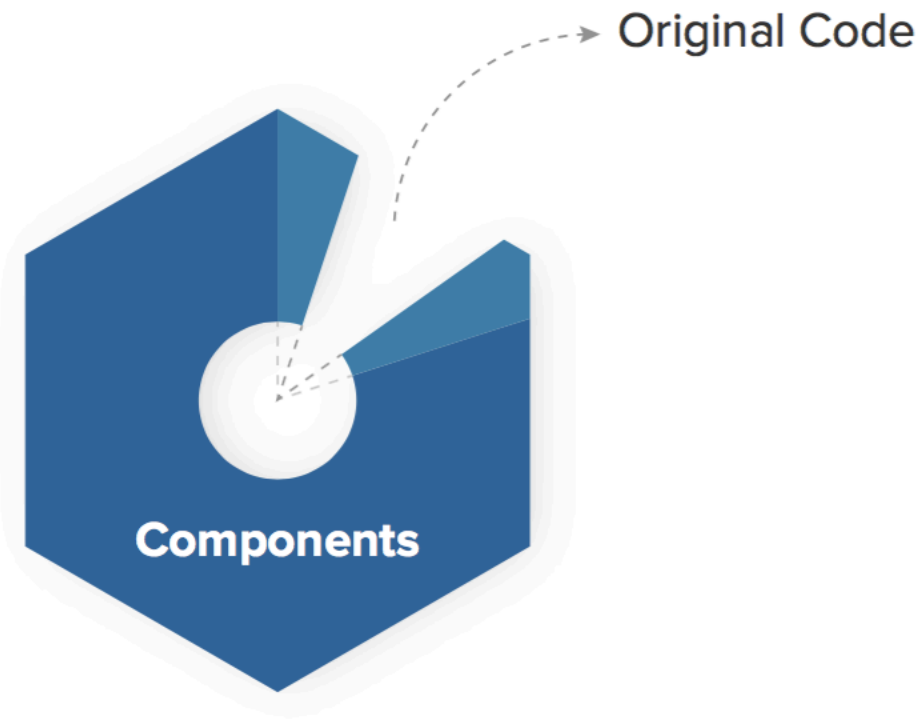
16,766,704

“Open source underpins all of our mission critical applications. Therefore, we must ensure that we are using the **highest quality components** at every stage of the development cycle.”

Don Duet

Co-head of Technology

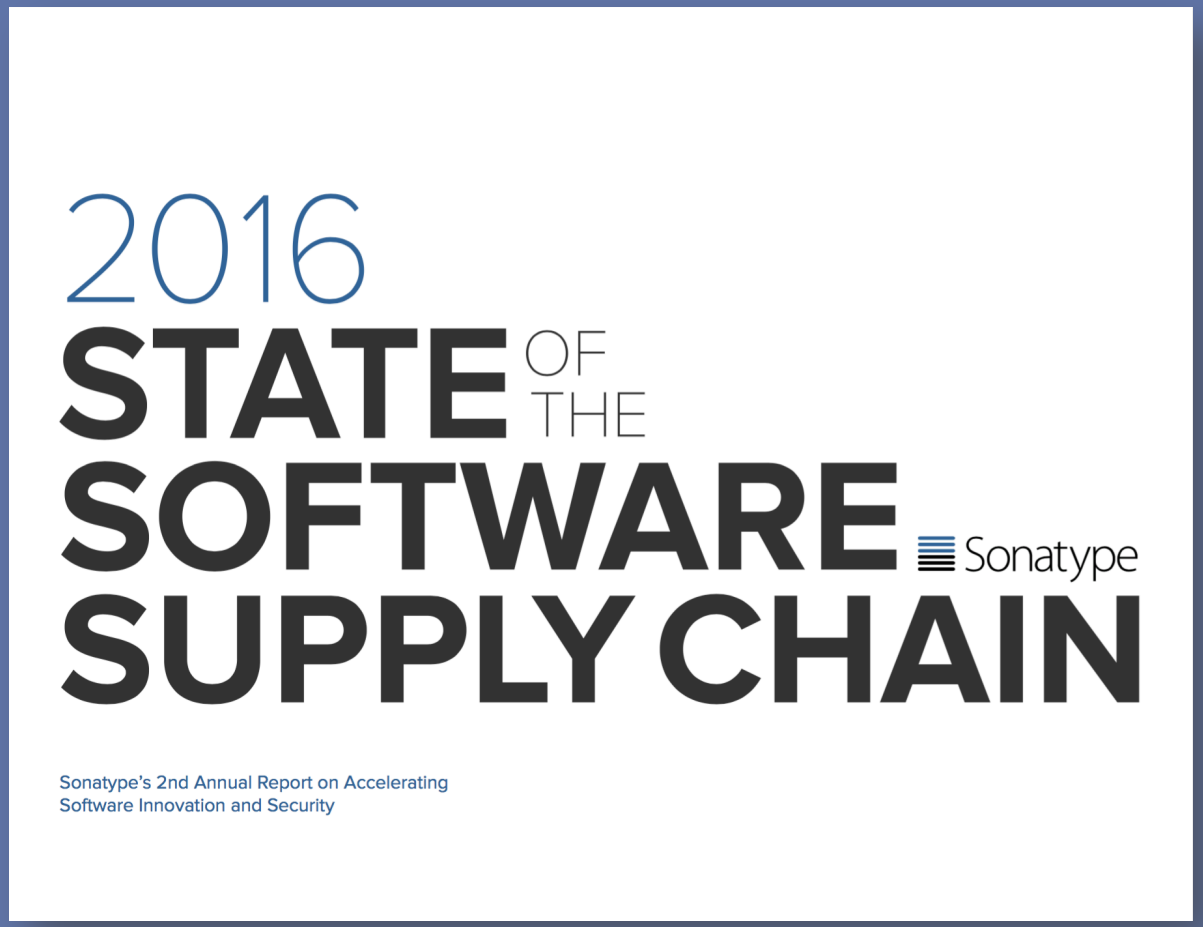
Goldman Sachs



80% to 90% of a typical application is composed of components.

SOFTWARE IS **MANUFACTURED** FROM PARTS

MASSIVE GAINS IN PRODUCTIVITY



3,000
organizations

25,000
applications

SAY HELLO TO YOUR SOFTWARE SUPPLY CHAIN

Sonatype

THE **BEST** ARE **BORROWING** FROM **DEMING**

Use fewer & better component suppliers

Use only the highest quality component parts

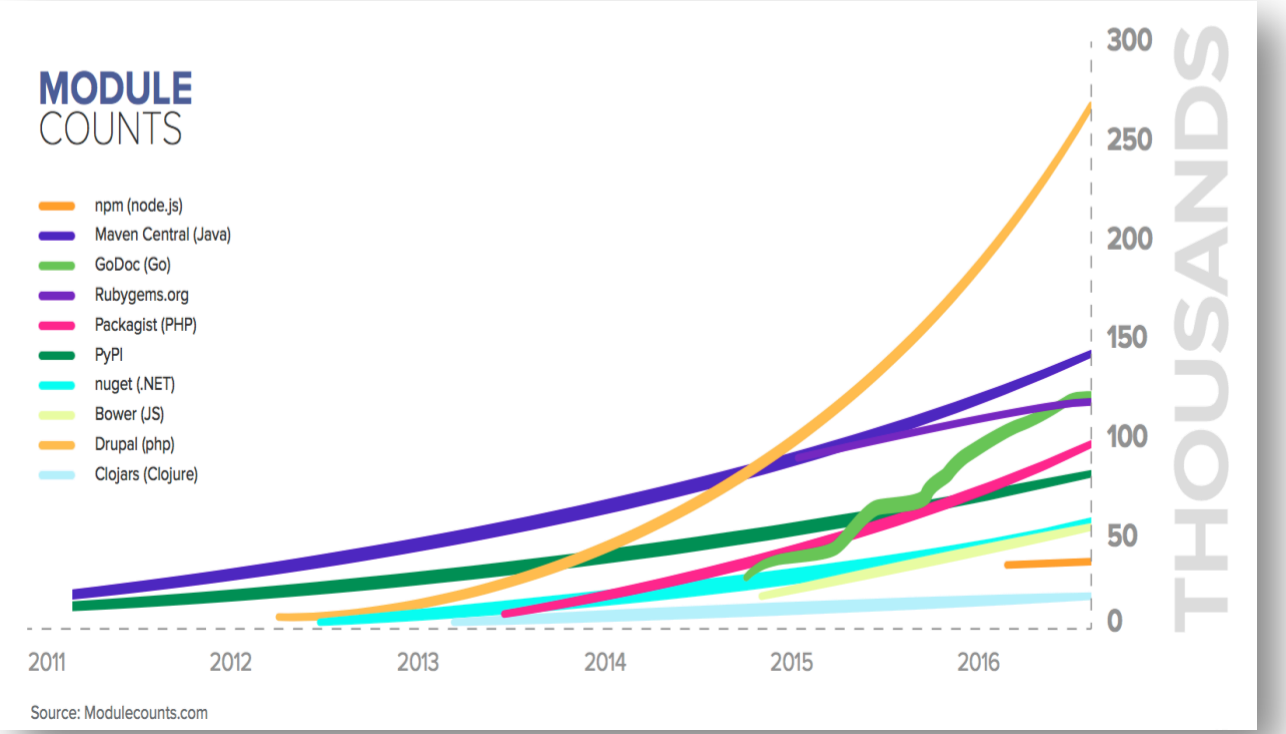
Continuously track when & where components are used

FEASTING ON A MASSIVE SUPPLY

1,000 new projects per day

10,000 new versions per day

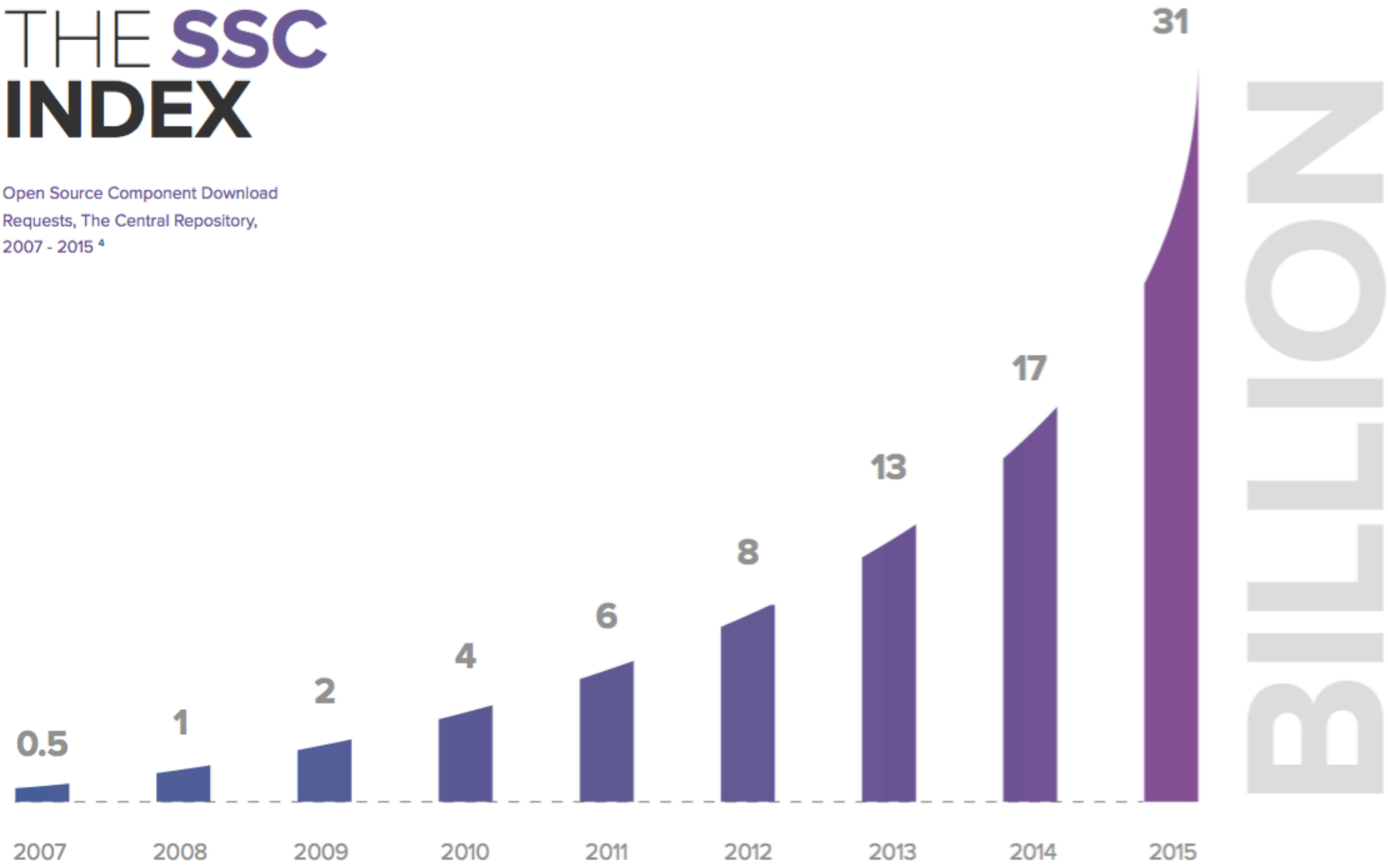
14x releases per year



@sonatype

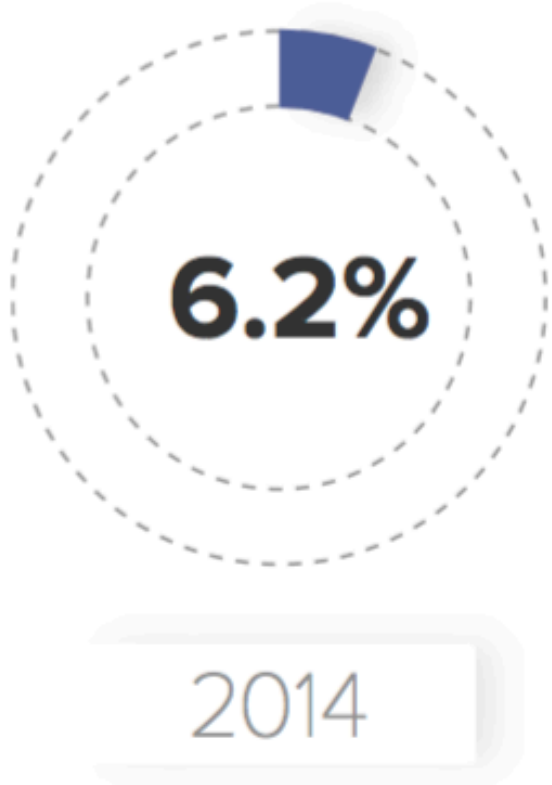
THE SSC INDEX

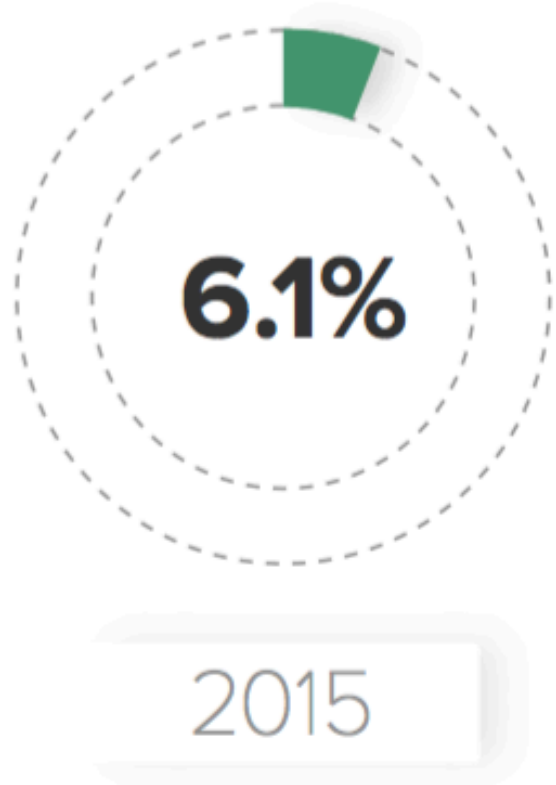
Open Source Component Download Requests, The Central Repository, 2007 - 2015 [4]



NOT **ALL** **PARTS** ARE **CREATED** **EQUAL**

SSC DEFECT DOWNLOAD RATIO





INNOVATION WAVE

IN YOUR SOFTWARE FACTORY

Analysis of 3,000 organizations

229,898

downloads

orders

5,275

components - all versions

parts

2,071

components

suppliers

Sonatype

Analysis of 3,000 organizations

229,898
downloads

17,206
7.48% known security vulnerabilities

Sonatype

Warehouses

6.1%
component downloads are vulnerable

Manufacturers

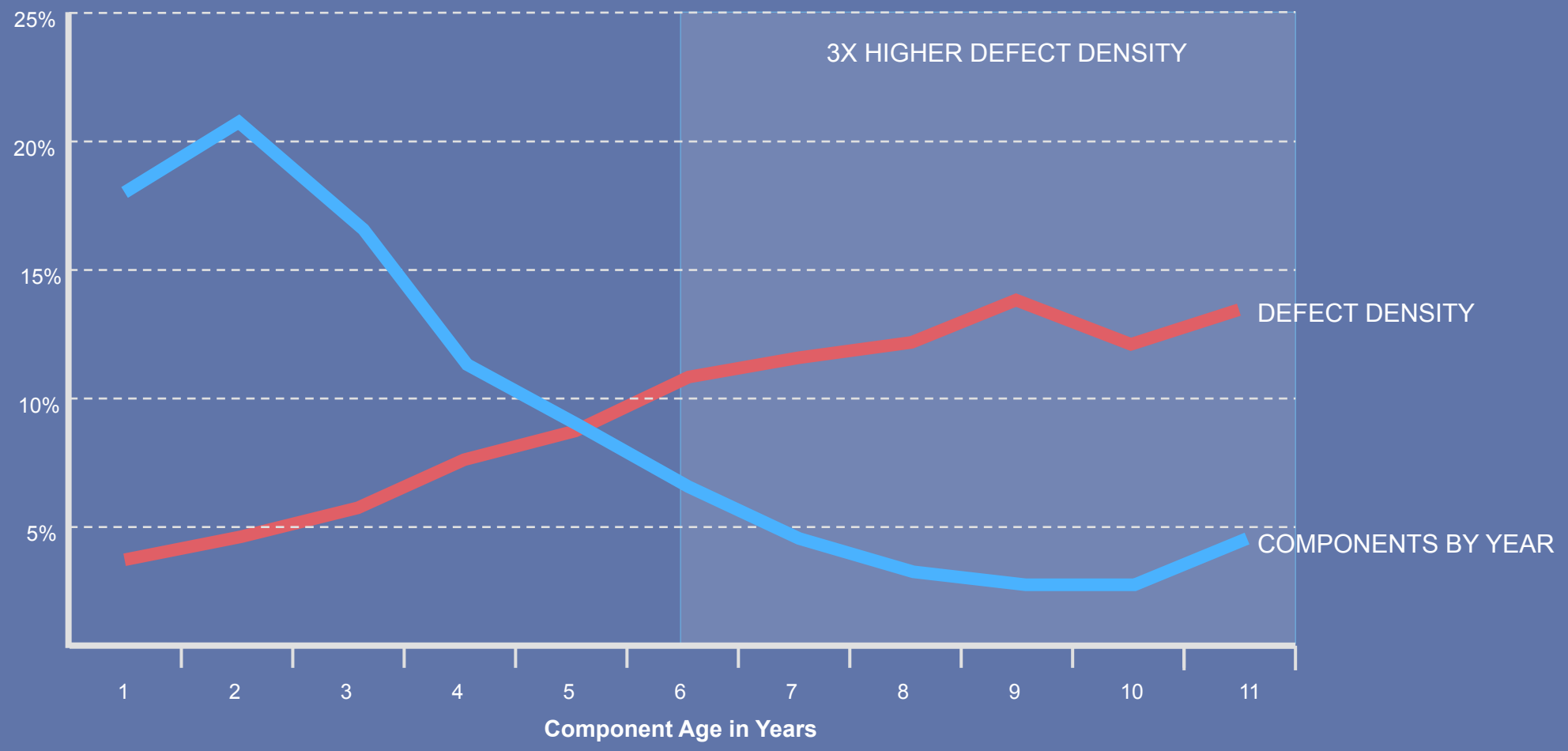
5.6%
components in repository managers are vulnerable

Finished Goods

6.8%
components in applications are vulnerable

NEWER **COMPONENTS** MAKE **BETTER SOFTWARE**

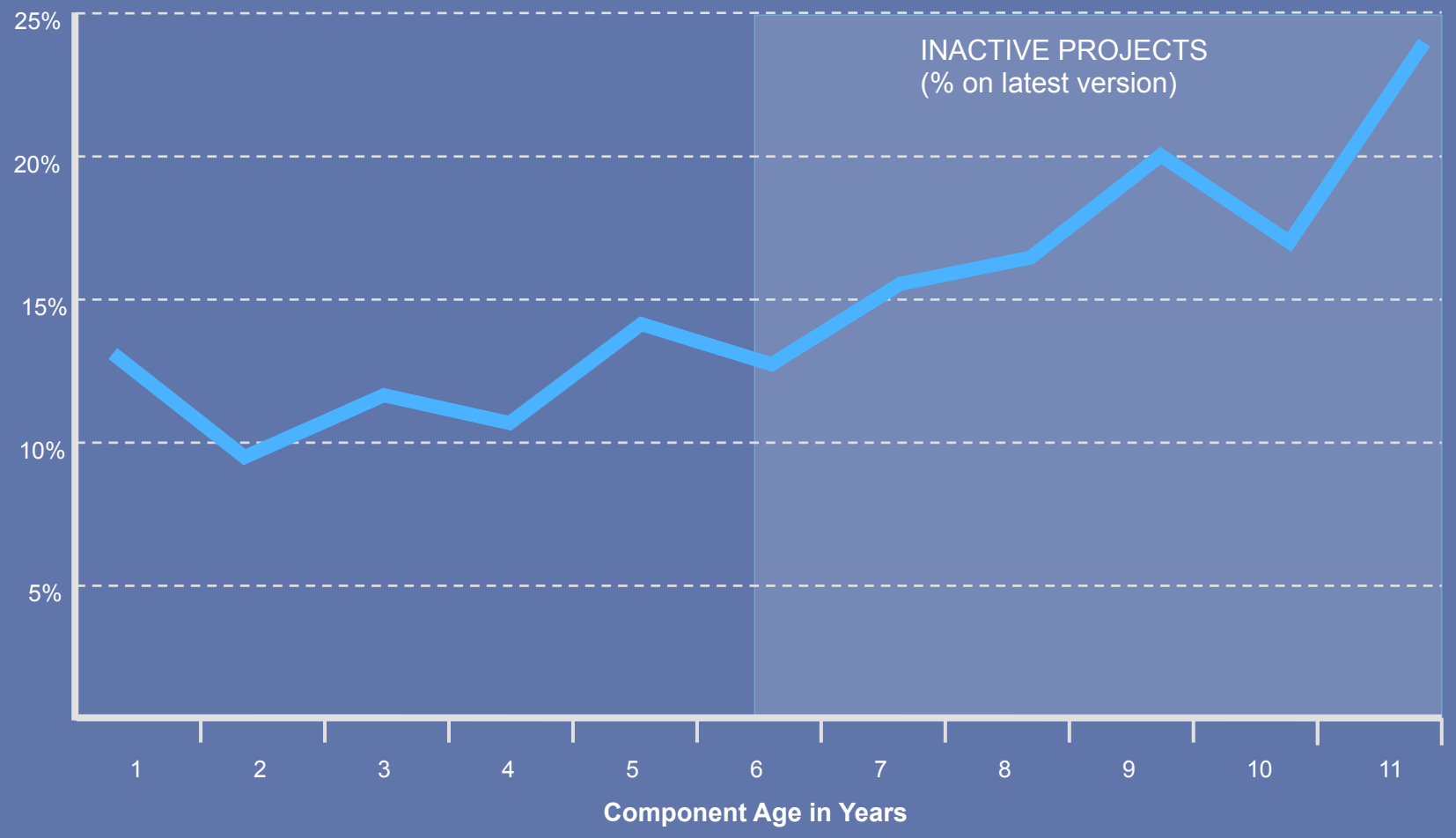
Analysis of components in 25,000 applications scans



Sonatype

OLDER COMPONENTS DIE OFF

Analysis of components in 25,000 applications scans

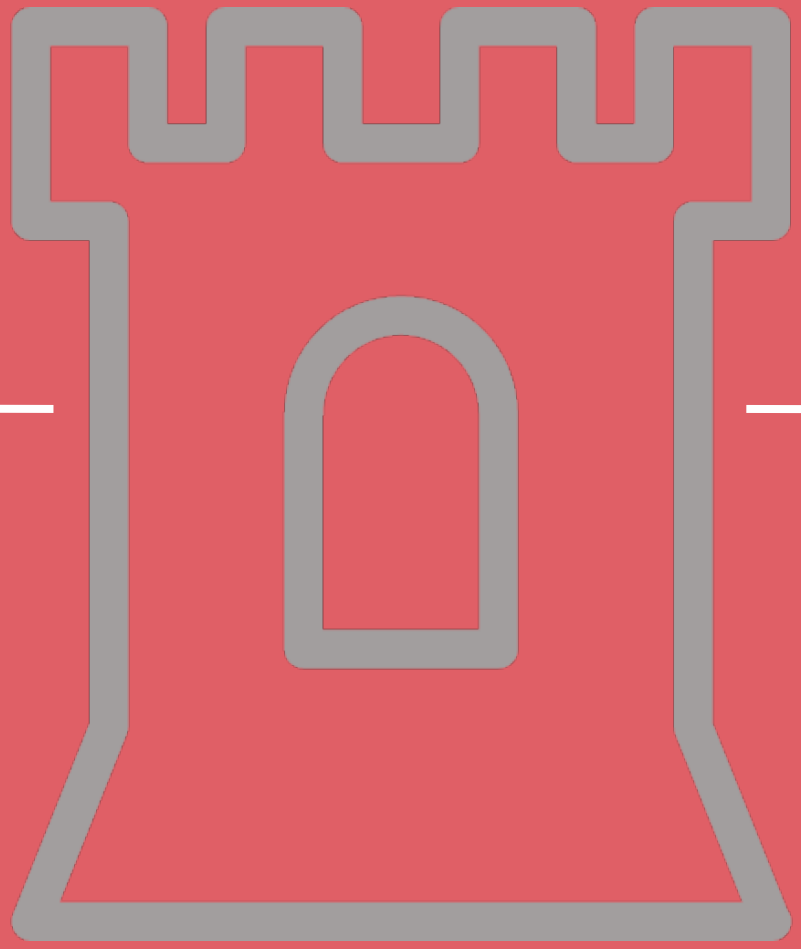


Sonatype

USE THE HIGHEST QUALITY PARTS

2007

CVE-2007-6721
CVSS Base Score: 10.0
HIGH
Impact Subscore: 10.0
Exploitability Subscore: 10.0



2015

8 years later, vulnerable versions of Bouncy Castle were downloaded…

5.8M times

PRACTICES ARE **GAINING TRACTION**

THE **NEW** RULES OF PROCUREMENT

Ingredients

Hygiene & Avoidable Risk

Remediation

MAYO CLINIC

UL

DEPARTMENT OF ENERGY · UNITED STATES OF AMERICA

FEDERAL TRADE COMMISSION · UNITED STATES OF AMERICA · MCMXV

18F

DEPARTMENT OF DEFENSE · UNITED STATES OF AMERICA

Exxon

OWASP
Open Web Application Security Project

FINANCIAL SERVICES ISAC

AMERICAN BANKERS ASSOCIATION

FREE software bill of materials

My Application - 2016-04-08 - *Release Report*

Summary | Policy | Security Issues | License Analysis

FILTER: All | Exact | Similar | Unknown | Proprietary

VIOLATIONS: Summary | All | Waived

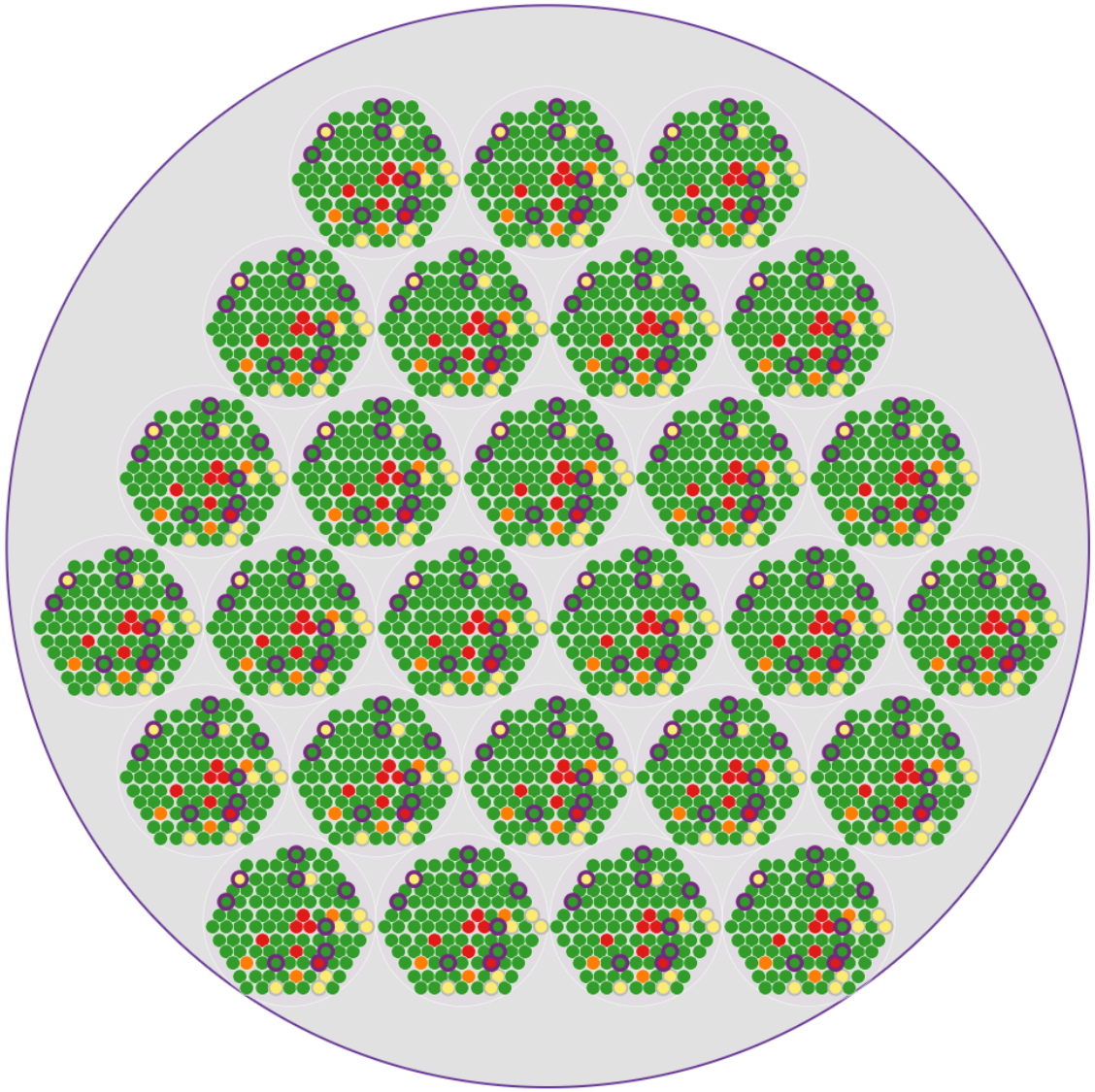
Policy Threat	Component	Popularity	Age	Release History
Search Name	Search Component			10 years
Security-High	org.apache.geronimo.framework : geronimo-secur...		8.2 y	
	org.mortbay.jetty : jetty : 6.1.15		7.1 y	
Security-Medium	org.openid4java : openid4java : 0.9.5		6.9 y	
	tomcat : catalina-host-manager : 5.5.23		8.3 y	
	tomcat : servlets-default : 5.5.4		10.5 y	
	tomcat : tomcat-util : 5.5.23		8.2 y	
None	ch.qos.logback : logback-access : 0.6		9.4 y	
	cobertura : cobertura : 1.6		10.4 y	
	commons-beanutils : commons-beanutils : 1.8.3		6.1 y	
	commons-dbcp : commons-dbcp : 1.4		6.2 y	
	commons-pool : commons-pool : 1.4		8.3 y	
	edu.stanford.ejalbert : BrowserLauncher2 : 1.3		4.6 y	
	edu.ucar : unidataCommon : 4.2.20		5.1 y	
	geronimo : geronimo-tomcat : 1.0		10.3 y	
	geronimo : geronimo-tomcat-builder : 1.1		9.5 y	

bit.ly/Sonatype_BOM

Sonatype

$7.42M

Estimated cost to remediate 10% of defects across 2000 applications.



www.sonatype.com/calculator

AUTOMATE AUTOMATE **AUTOMATE**

@sonatype

CASE STUDY: Global Insurer

1. Reduce defects from 10 per 10,000 lines of code
2. Reduce rework and improve productivity by 15%

CASE STUDY: Global Insurer

Use fewer & better component suppliers

from
10 to 4

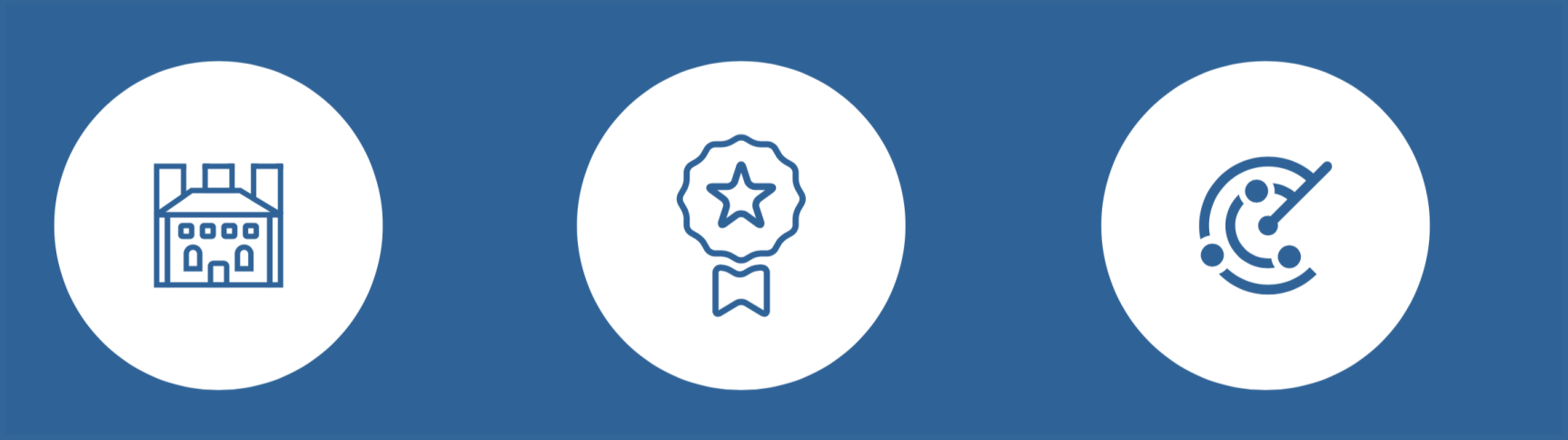
Use only the highest quality component parts

from
4 to 1

Continuously track when & where components are used

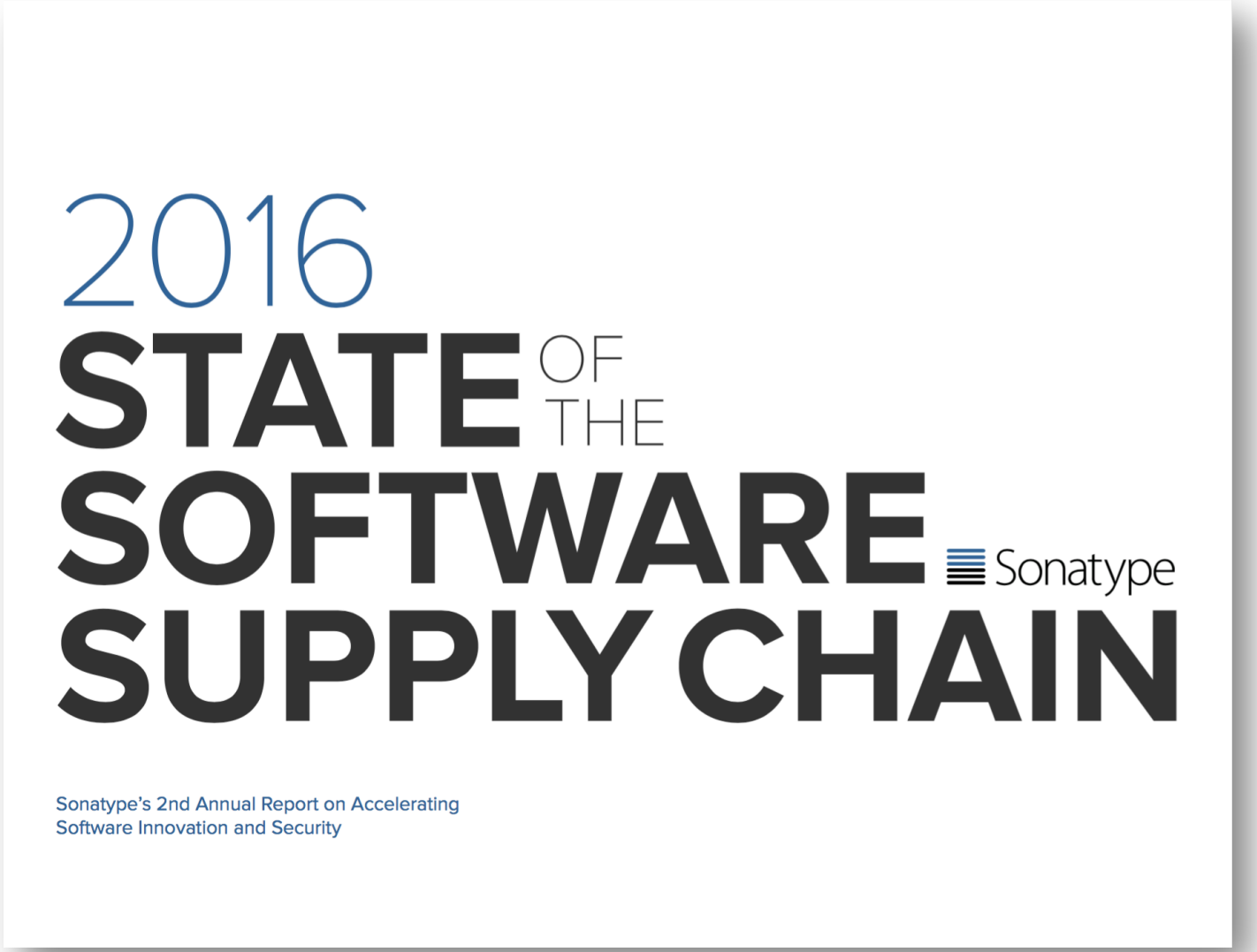
use software
bill of materials

CASE STUDY: Global Insurer



Developers are 30% more productive.

Get the report today.



www.sonatype.com/ssc2016

Sonatype

MEETUPS, CONFERENCES, **USER GROUPS**

weeks@sonatype.com

Sonatype

EMPOWER DEVELOPERS FROM THE START

ZTTR (Zero Time to Remediation)

Sonatype

DESIGN A FRICTIONLESS APPROACH

Sonatype Nexus Professional | CLM Management | Dashboard [Jenkins] | CLM Report

http://localhost:8060

Most Visited | Large Persistent C... | Google | Getting Started | Sonatype Nexus P... | System Dashboar...

Jenkins

search

Jenkins

ENABLE AUTO REFRESH

- New Item
- People
- Build History
- Project Relationship
- Check File Fingerprint
- Manage Jenkins
- Credentials

Build Queue

No builds in the queue.

Build Executor Status

1 Idle
2 Idle

add description

All +

S	W	Name ↓	Last Success	Last Failure	Last Duration	Policy Violations
		Enterprise App Snap with Nexus Pro Staging	2 mo 3 days - #85	25 min - #88	1 min 10 sec	5 4 31
		EnterpriseApp1	3 mo 23 days - #107	21 min - #134	2 min 9 sec	10 5 33
		Hadoop	N/A	3 mo 1 day - #25	2 min 41 sec	6
		Ozone Widget Framework	N/A	7 days 3 hr - #10	55 sec	
		WebgoatSrc	6 days 3 hr - #71	6 min 22 sec - #73	40 sec	5 5 29

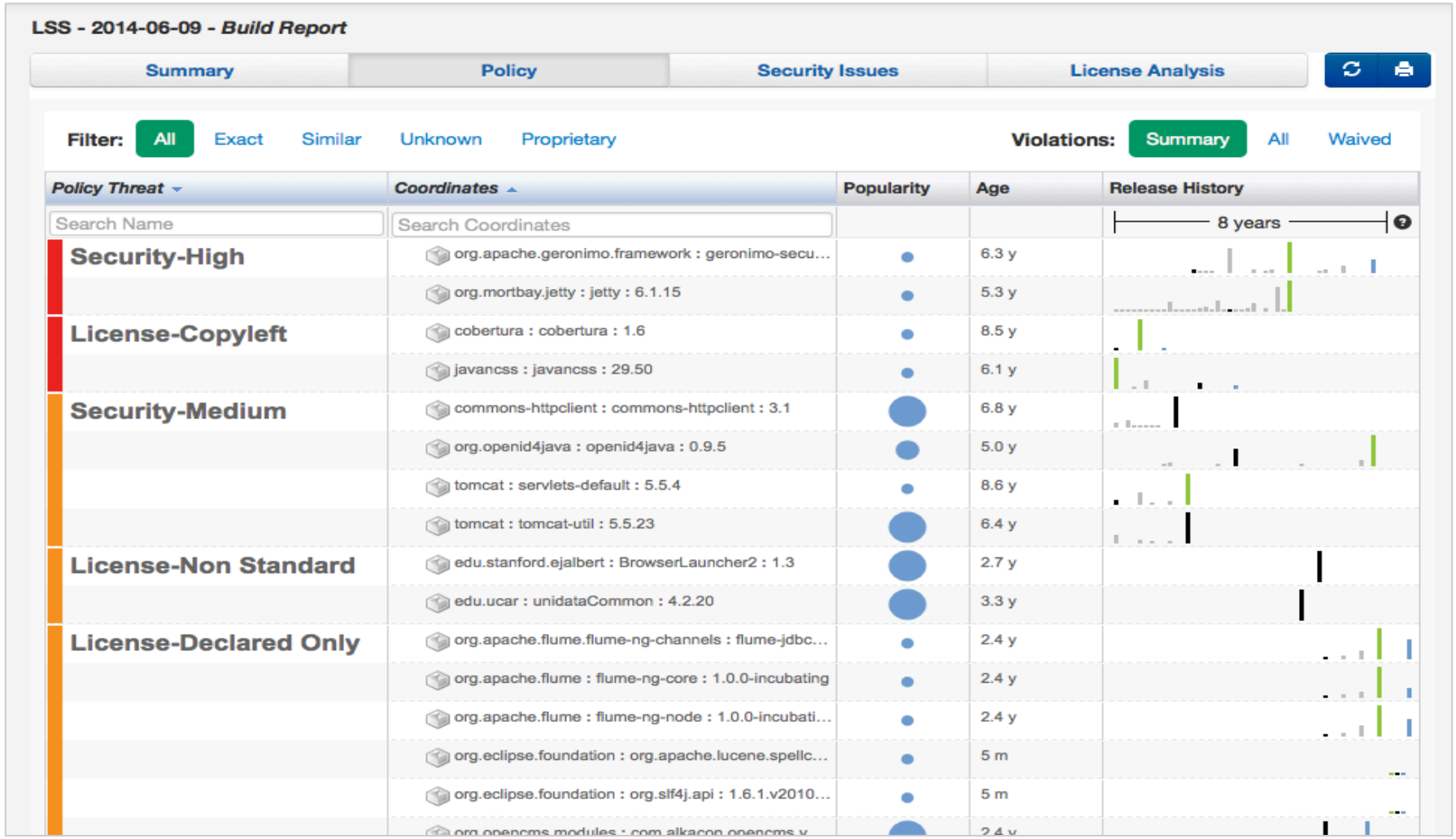
Icon: S M L

Legend | RSS for all | RSS for failures | RSS for just latest builds

Help us localize this page

Page generated: Dec 16, 2014 1:23:31 PM | REST API | Jenkins ver. 1.589

CREATE A SOFTWARE BILL OF MATERIALS



bit.ly/softwareBOM