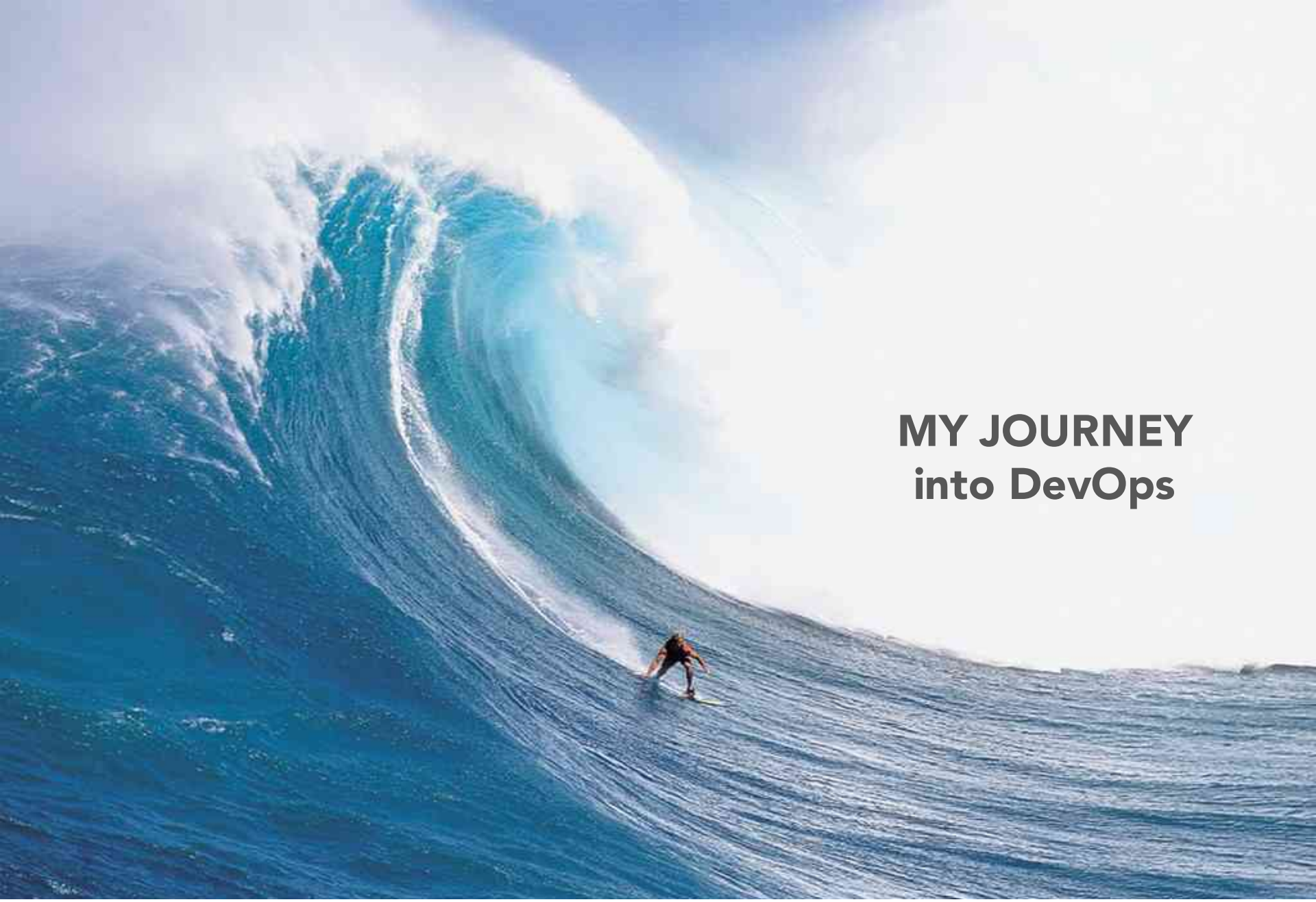
The Illusion of Control:

Secrets Within Your Software Supply Chain

Derek E. Weeks
VP and Rugged DevOps Advocate
@weekstweets

Trust me. It's not *all* about

SECURITY.



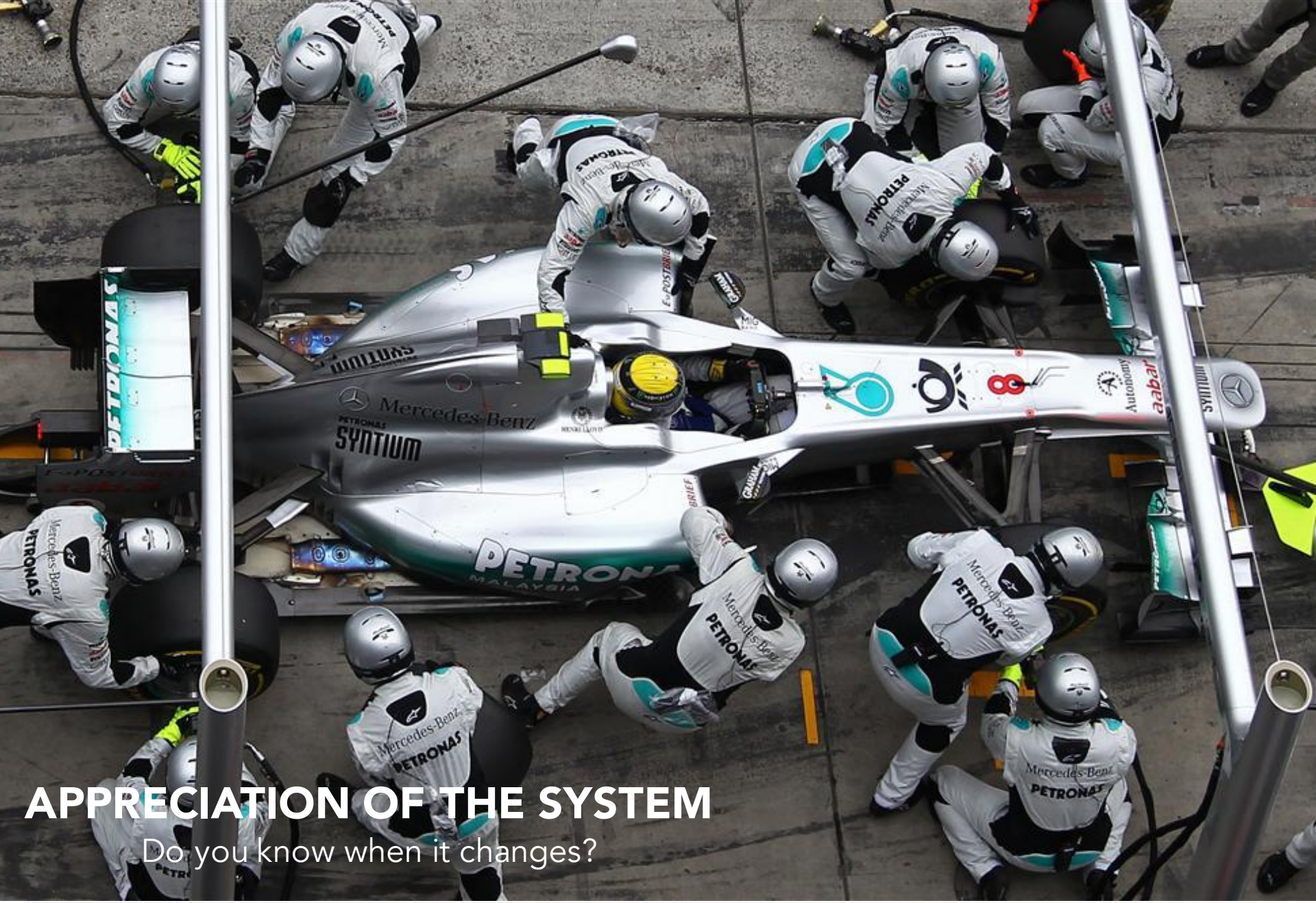
Sonatype

HIGH PERFORMERS

Where do they come from?

APPRECIATION OF THE SYSTEM

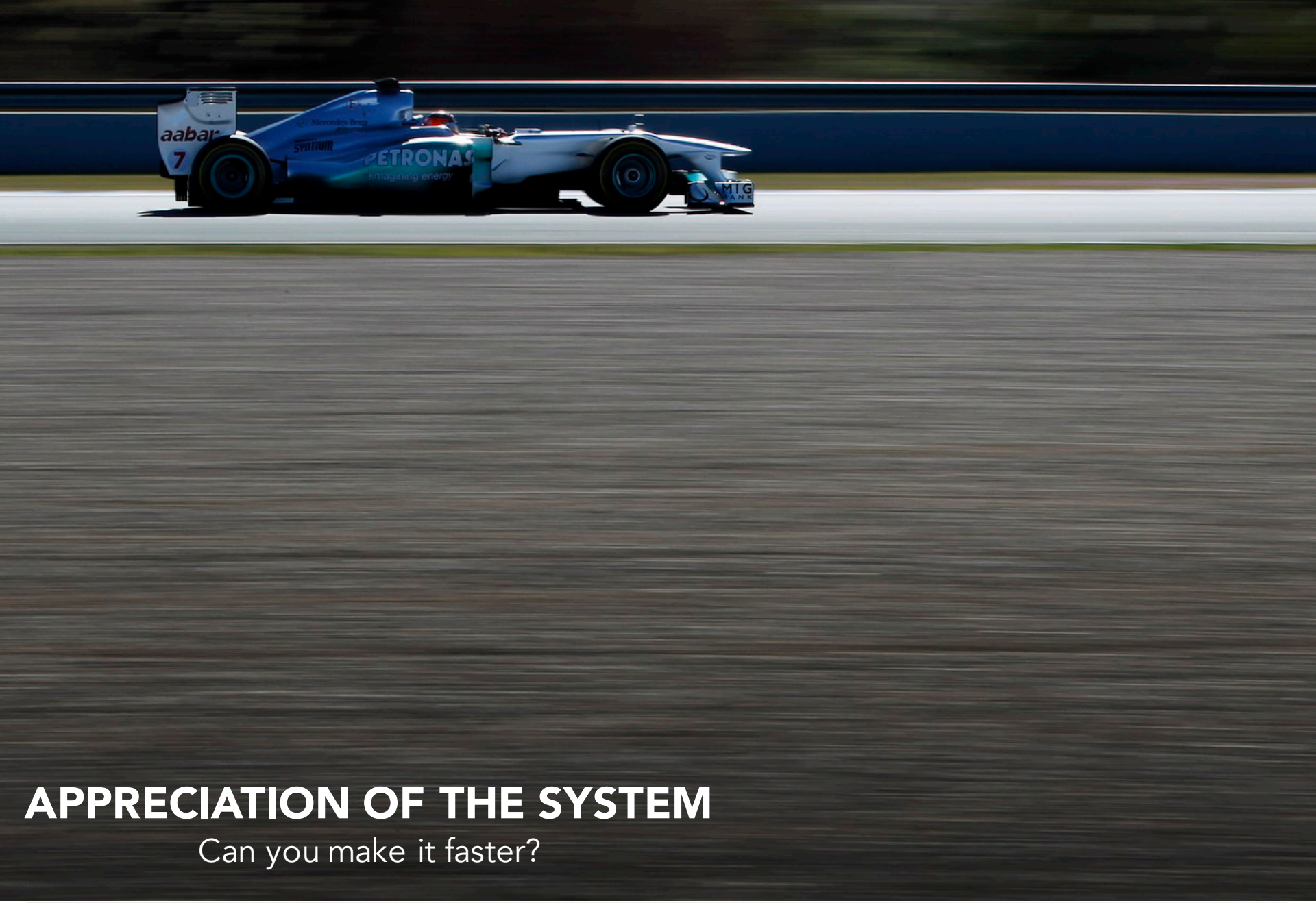
Do you know what you have?



APPRECIATION OF THE SYSTEM

Do you know when it changes?

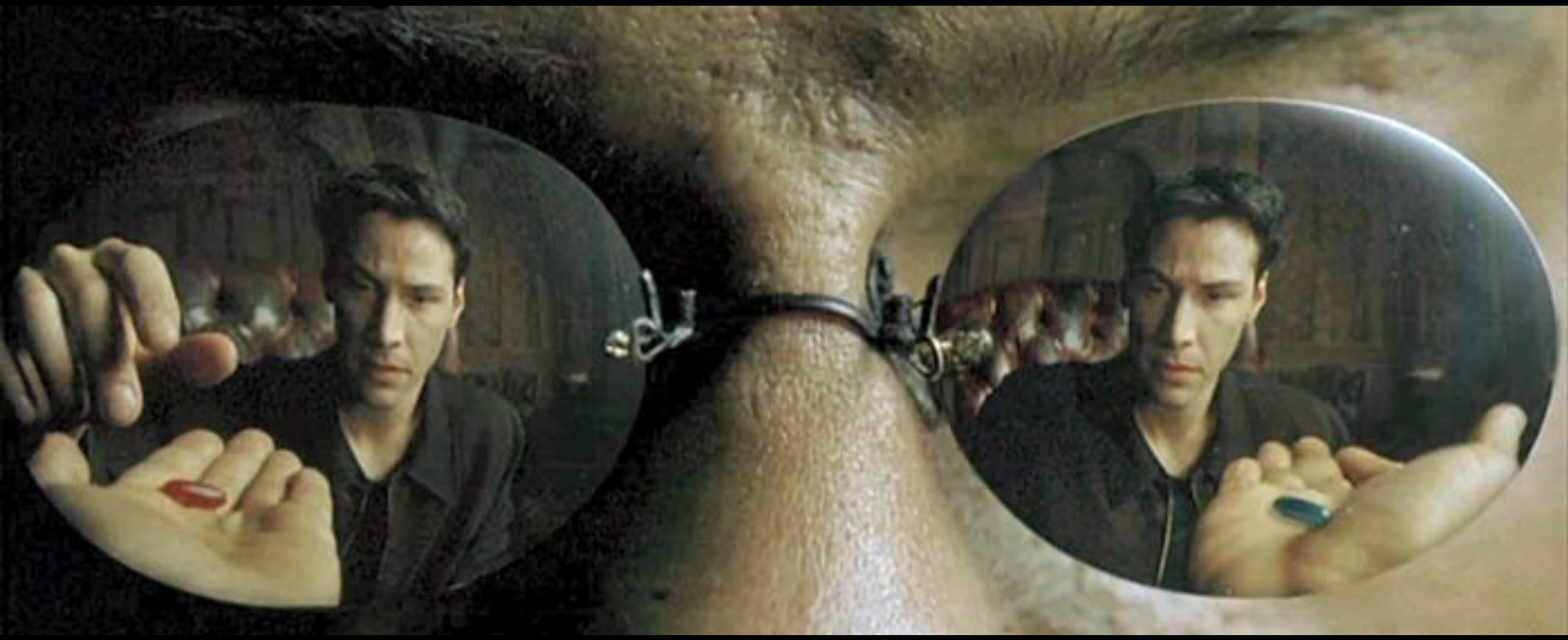
Sonatype



APPRECIATION OF THE SYSTEM

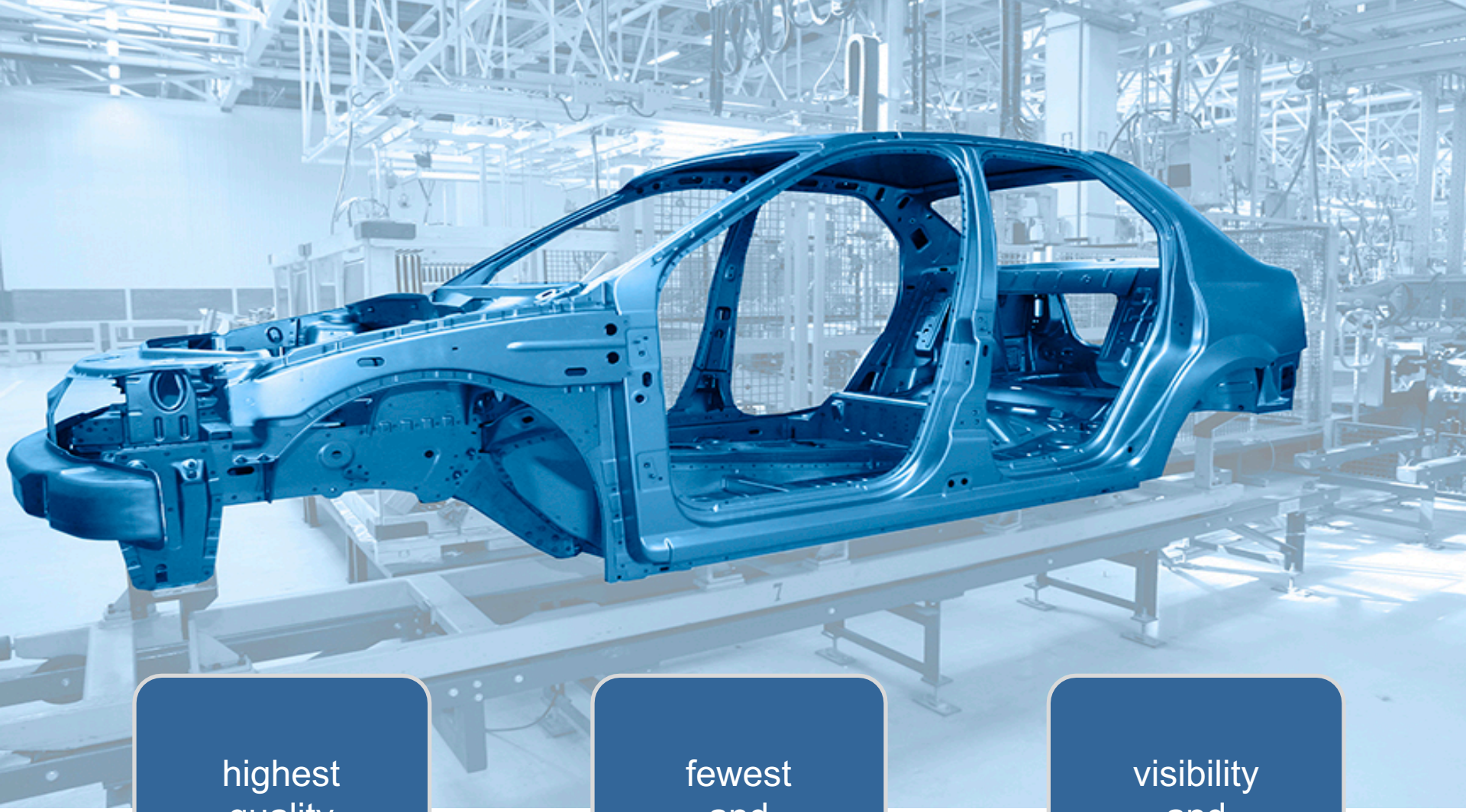
Can you make it faster?

Sonatype



YOUR REWARD

More Innovation.
Less Rework.



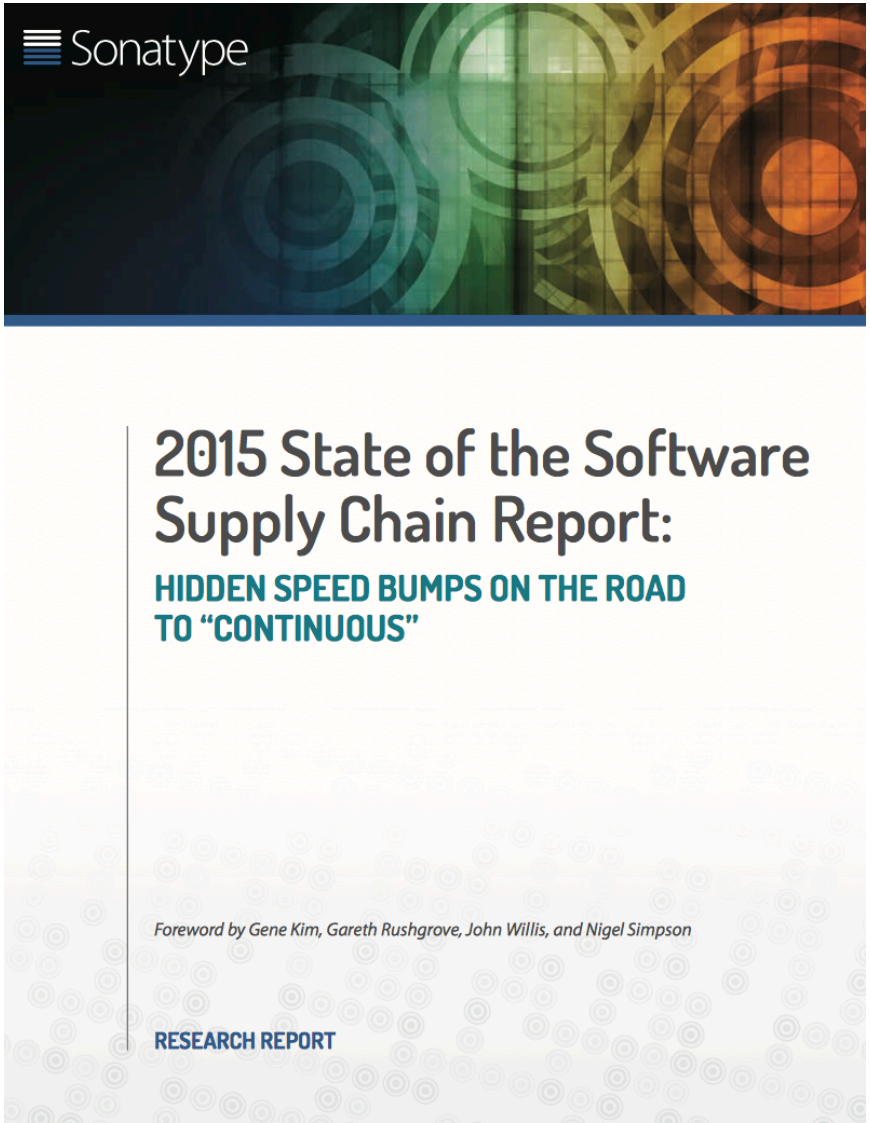
highest quality parts

fewest and best suppliers

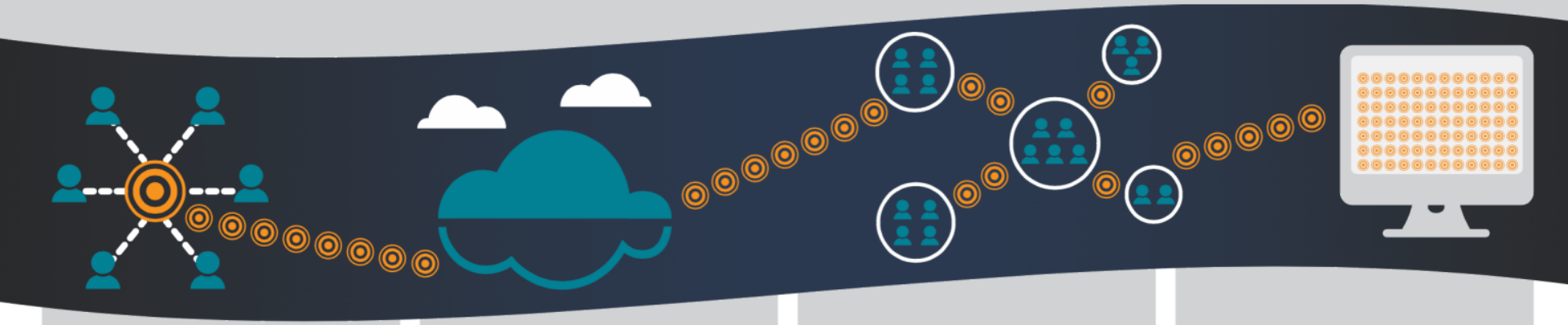
visibility and traceability

106,000

Organizations Analyzed



Source: 2015 State of the Software Supply Chain Report



SUPPLIERS
Open Source Projects

WAREHOUSES
Component Repositories

MANUFACTURERS
Software Development Teams

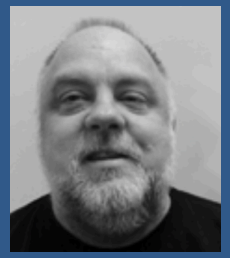
FINISHED GOODS
Software Applications

We all have a

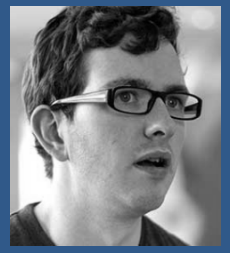
SOFTWARE SUPPLY CHAIN

Modern software development **HAS CHANGED**

Our process **HASN'T CHANGED ENOUGH**



John Willis
Docker



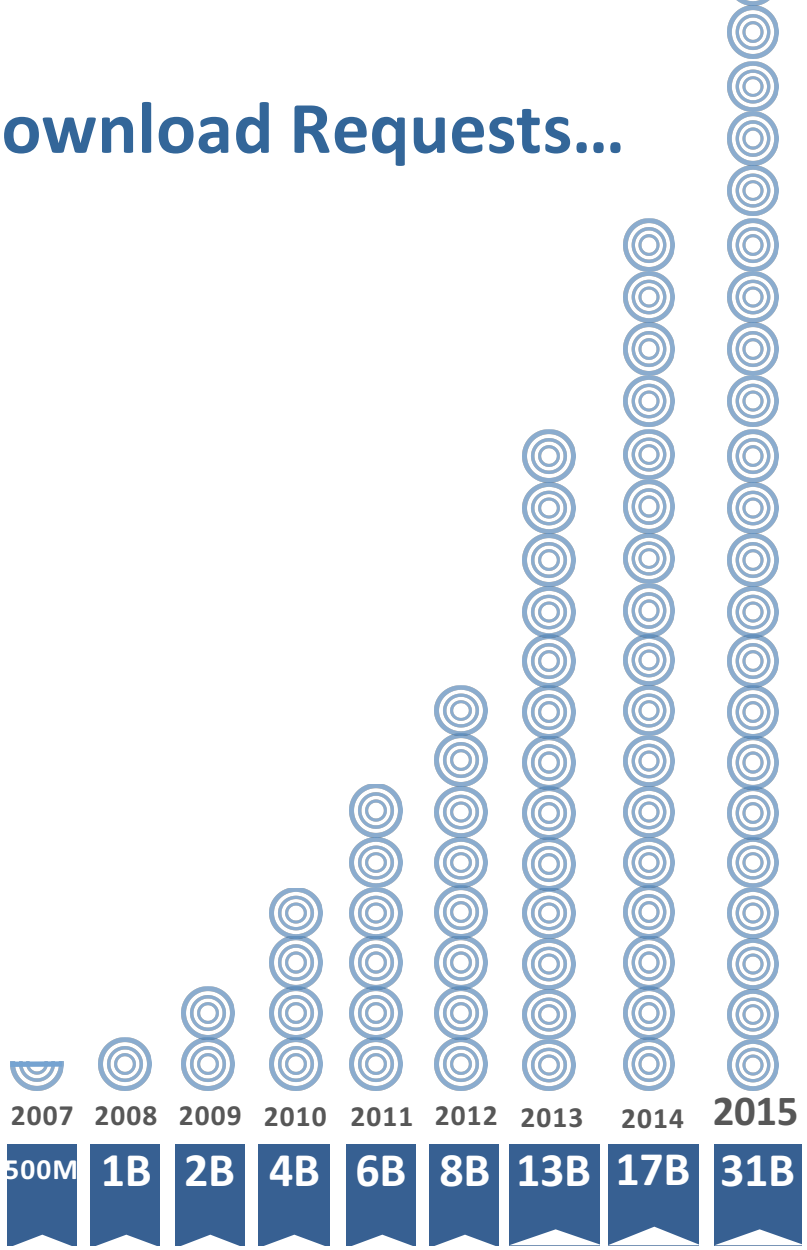
Gareth Rushgrove
Puppet Labs

Nigel Simpson
Disney

"Just as in manufacturing, the effective management of our supply chains will create **WINNERS** and **LOSERS**"

Gene Kim, Co-author of "The Phoenix Project: A Novel About IT, DevOps, and Helping Your Business Win" and upcoming "DevOps Cookbook"

Open Source Download Requests…



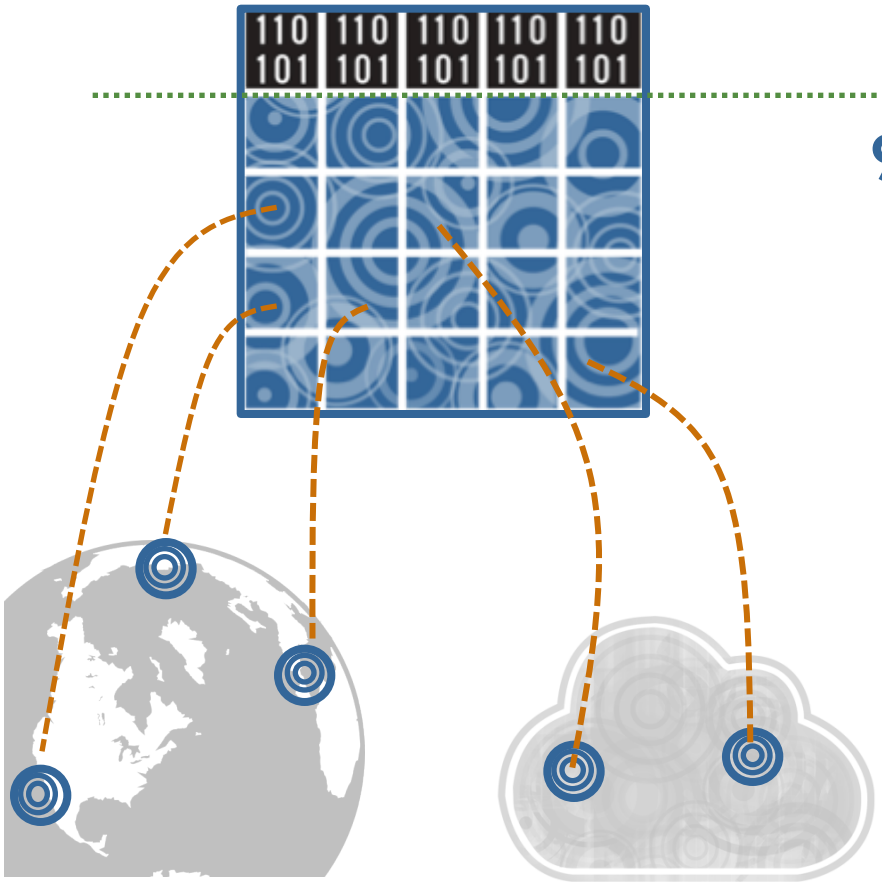
POLLING QUESTION

What percent of modern apps are composed of open source components?

a. 10 - 20%
b. 50 - 60%
c. 80 - 90%

How Dependent on 3rd Parties Are We?

Typical Application



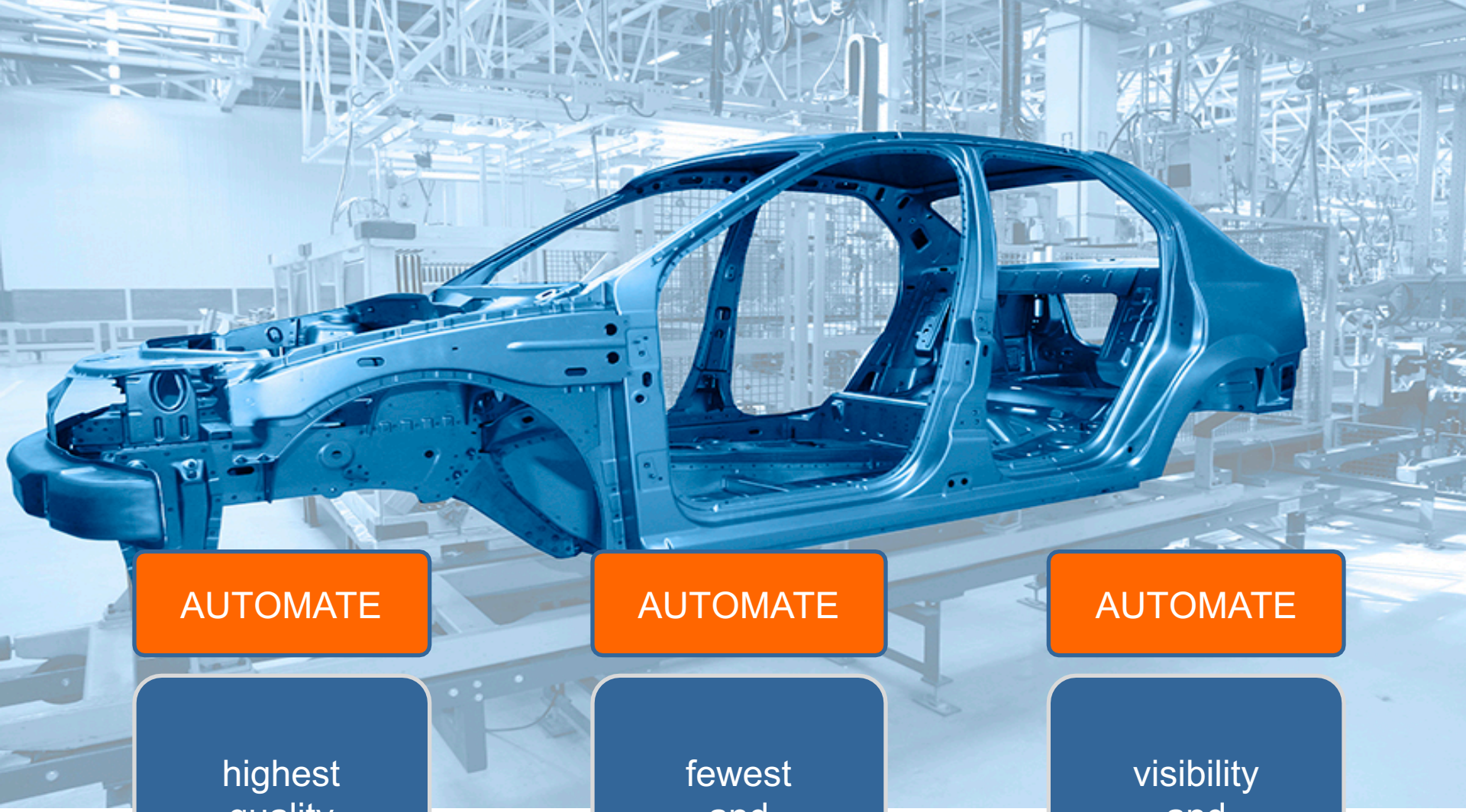
10% Custom Written Code

90% From 3rd Parties

Open Source

Closed Source

Cloud Services



AUTOMATE

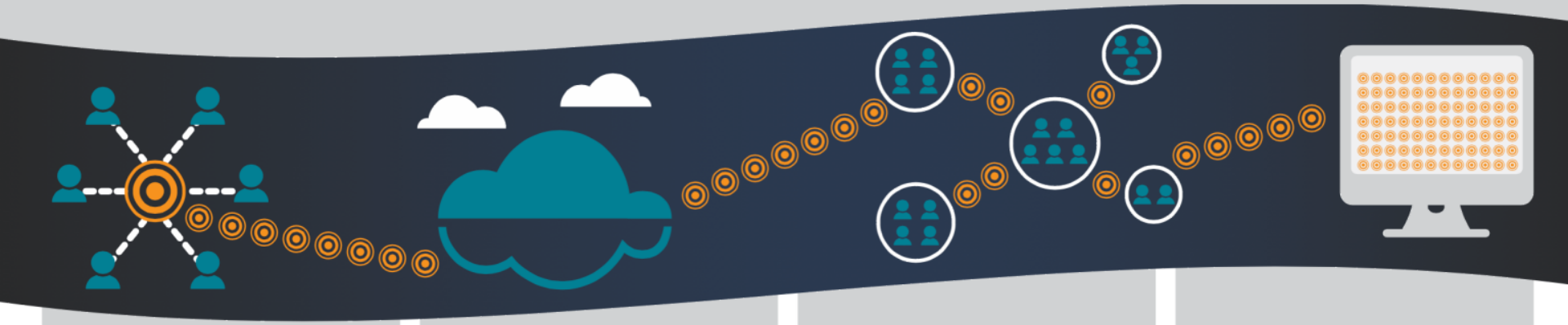
highest quality parts

AUTOMATE

fewest and best suppliers

AUTOMATE

visibility and traceability

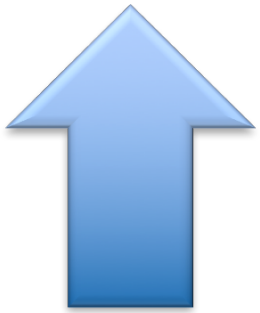


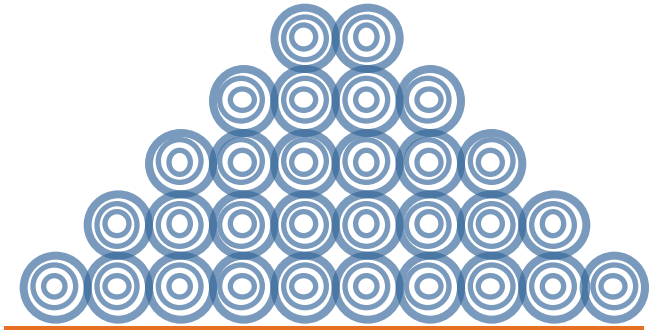
SUPPLIERS
Open Source Projects

WAREHOUSES
Component Repositories

MANUFACTURERS
Software Development Teams

FINISHED GOODS
Software Applications





1,208,005 OSS COMPONENTS

CHANGE

Typical component is updated 3 - 4X per year.

130,086 SUPPLIERS

11 MILLION OSS USERS

Source: 2015 State of the Software Supply Chain Report

POLLING QUESTION

How many open source suppliers do companies work with?

a. 5,372
b. 7,601
c. 15,118

Suppliers Serving Manufacturers

	Orders (downloads)	**Suppliers** (artifacts)	**Parts** (versions)
Average	240,757	7,601	18,614

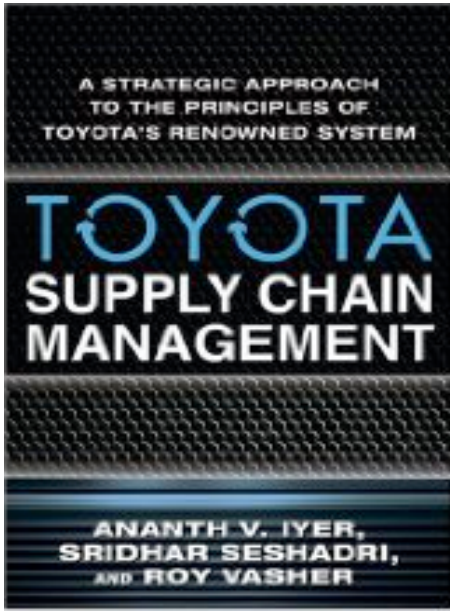
Source: 2015 State of the Software Supply Chain Report

too much

WIP

Comparing the Prius and the Volt

	Toyota Advantage	Toyota Prius	Chevy Volt
Unit Cost	61%	$24,200	$39,900
Units Sold	13x	23,294	1,788
In-House Production	50%	27%	54%
Plant Suppliers	16% (10x per)	125	800
Firm-Wide Suppliers	4%	224	5,500



COLUMNS

Almost Too Big to Fail

DAN GEER AND JOSHUA CORMAN

Dan Geer is the CISO for In-Q-Tel and a security researcher with a quantitative bent. He has a long history with the USENIX Association, including officer positions, program committees, etc. dan@geer.org

Joshua Corman is the chief technology officer for Sonatype. Previously, Corman served as a security researcher and strategist at Akamai Technologies, The 451 Group, and IBM Internet Security Systems. A respected innovator, he co-founded Rugged Software and I Am the Cavalry to encourage new security approaches in response to the world's increasing dependence on digital infrastructure. He is also an adjunct faculty for Carnegie Mellon's Heinze College, IANS Research, and a Fellow at the Ponemon Institute. Josh received his bachelor's degree in philosophy, graduating summa cum laude, from the University of New Hampshire. joshcorman@gmail.com

Both dependence on open source and adversary activity around open source are widespread and growing, but the dynamic pattern of use requires new means to estimate if not bound the security implications. In April and May 2014, every security writer has talked about whether it is indeed true that with enough eyeballs, all bugs are shallow. We won't revisit that topic because there may be no minds left to change. Unarguably:

- Dependence on open source is growing in volume and variety.
- Adversary interest tracks installed base.
- Multiple levels of abstraction add noise to remediation needs.

We begin with two open source examples.

Apache Struts CVE-2013-2251, July 6, 2013 - CVSS v2 9.3

Apache Struts is one of the most popular and widely depended upon open source projects in the world. As such, when this highly exploitable vulnerability was discovered, it was promptly used to compromise large swaths of the financial services sector. While Heartbleed (see below) got full media frenzy, many affected by 2013-2251 learned of the problem from FBI victim notifications under 42 U.S.C. § 10607. The FS-ISAC issued guidance [1] telling institutions (read, victims) to scrutinize the security of third-party and open source components throughout their life cycle of use. It is not noteworthy that an open source project could have a severe vulnerability; what *is* of note is that this flaw went undetected for at least seven years (if not a lot longer from WebWork 2/pre-Struts 2 code base)—an existence proof that well-vetted code still needs a backup plan.

OpenSSL (Heartbleed) CVE-2014-0160, April 7, 2014 - CVSS v2 5.0

The Heartbleed vulnerability in OpenSSL garnered tremendous media and attacker activity this past April. While only scored with a CVSS of 5.0, it is a "5 with the power of a 10" since sniffing usernames, passwords, and SSL Certificates provides stepping stones to far greater impact. In contrast to the Struts bug above, this flaw was introduced only two years prior, but it, too, went unnoticed by many eyeballs—it was found by bench analysis [2].

Dependence on Open Source Is Growing

Sonatype, home to author Corman, serves as custodian to Central Repository, the largest parts warehouse in the world for open source components. At the macro level, open source consumption is exploding in Web applications, mobility, cloud, etc., driven in part by increasingly favorable economics. Even (risk averse, highly regulated) government and financial sectors, which previously resisted "code of unknown origin/quality/security," have begun relaxing their resistance. According to both Gartner surveys and Sonatype application analysis, 90+% of modern applications are not so much written as assembled from third-party building blocks. It is the open source building blocks that are taking the field, and not just for commodity applications (see Figure 1).

59%

never repaired

41%

390 days (median 265 days). CVSS 10s 224 days

<7

The best were remediated in under a week.

Source: USENIX, https://www.usenix.org/system/files/login/articles/15_geer_0.pdf

SUPPLIERS
Open Source Projects

November 6, 2015

What Do WebLogic, WebSphere, JBoss, Jenkins, OpenNMS, and Your Application Have in Common? This Vulnerability.

By @breenmachine

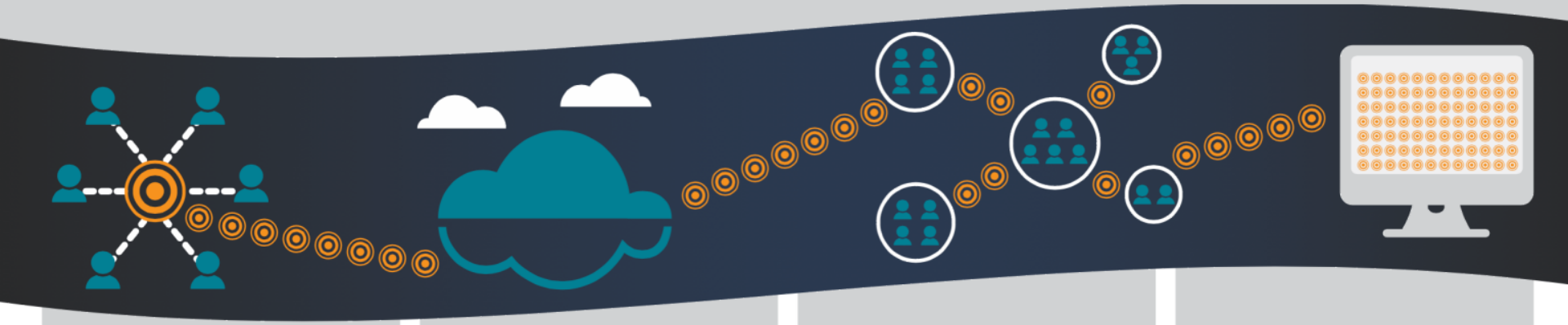
What?

The most underrated, underhyped vulnerability of 2015 has recently come to my attention, and I'm about to bring it to yours. No one gave it a fancy name, there were no press releases, nobody called Mandiant to come put out the fires. In fact, even though proof of concept code was released OVER 9 MONTHS AGO, none of the products mentioned in the title of this post have been patched, along with many more. In fact no patch is available for the Java library containing the vulnerability. In addition to any commercial products that are vulnerable, this also affects many custom applications.

In this post I'll be dropping pre-authentication, remote code execution exploits that leverage this vulnerability for WebLogic, WebSphere, JBoss, Jenkins, and OpenNMS. All on the newest versions. Even more interesting, I'll detail the process we went through to discover that these products were vulnerable, and how I developed the exploits. This should empower you to go out and find this same bug in your own software or commercial products that you or your clients use. All code can be found on the FoxGlove Security Github.

I'll also be touching on why this bug is unlikely to go away soon. You can infuriate your developers and ops people by telling them to follow the instructions in "The Fix" section to remediate this in your environment. It will fix it, but it's an admittedly ugly solution.

This post is going to be long. Because I'm a nice person, I made you an index. Feel free to skip straight to the exploits if you've got better things to do than read my rambling:

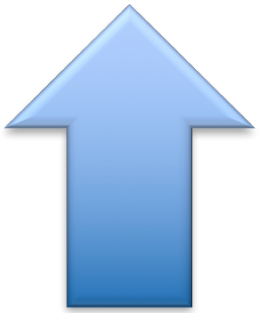


SUPPLIERS
Open Source Projects

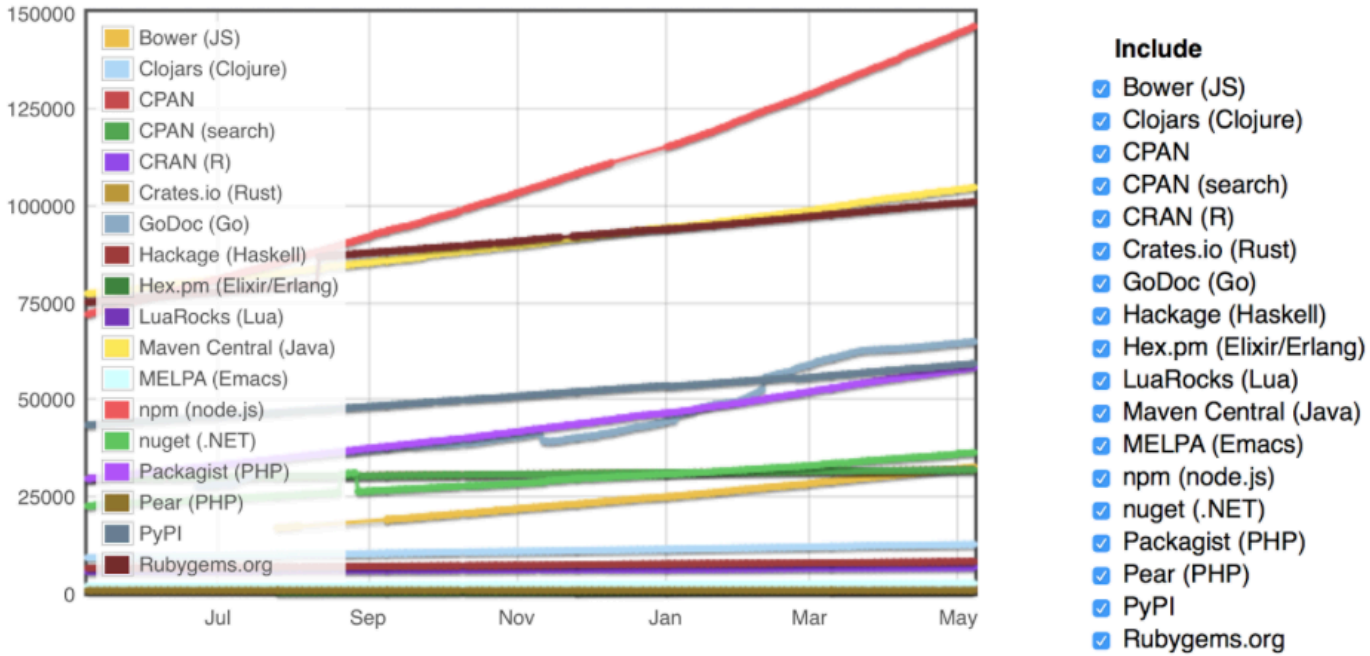
WAREHOUSES
Component Repositories

MANUFACTURERS
Software Development Teams

FINISHED GOODS
Software Applications



Module Counts



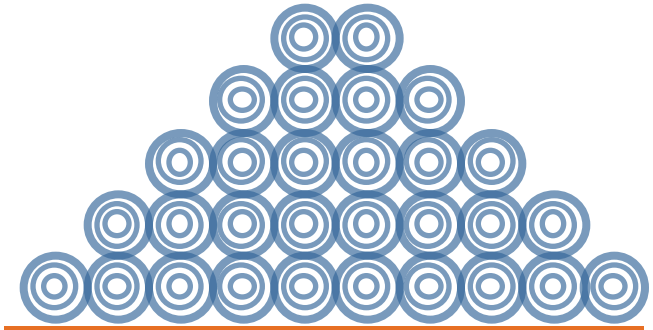
Growth in open source projects, 2014 - 2015[3]

Source: modulecounts.com

Sample of **Open Source Repositories**	2014 **Volume of Download Requests**
Central.sonatype.org	17,213,084,947
Npmjs.org	15,460,748,856
NuGetGallery.com	280,124,916
Bintray.com	250,000,000

Source: 2015 State of the Software Supply Chain Report

WAREHOUSES
Component Repositories



1,208,005 OSS COMPONENTS

CHANGE

Typical component is updated 3 - 4X per year.

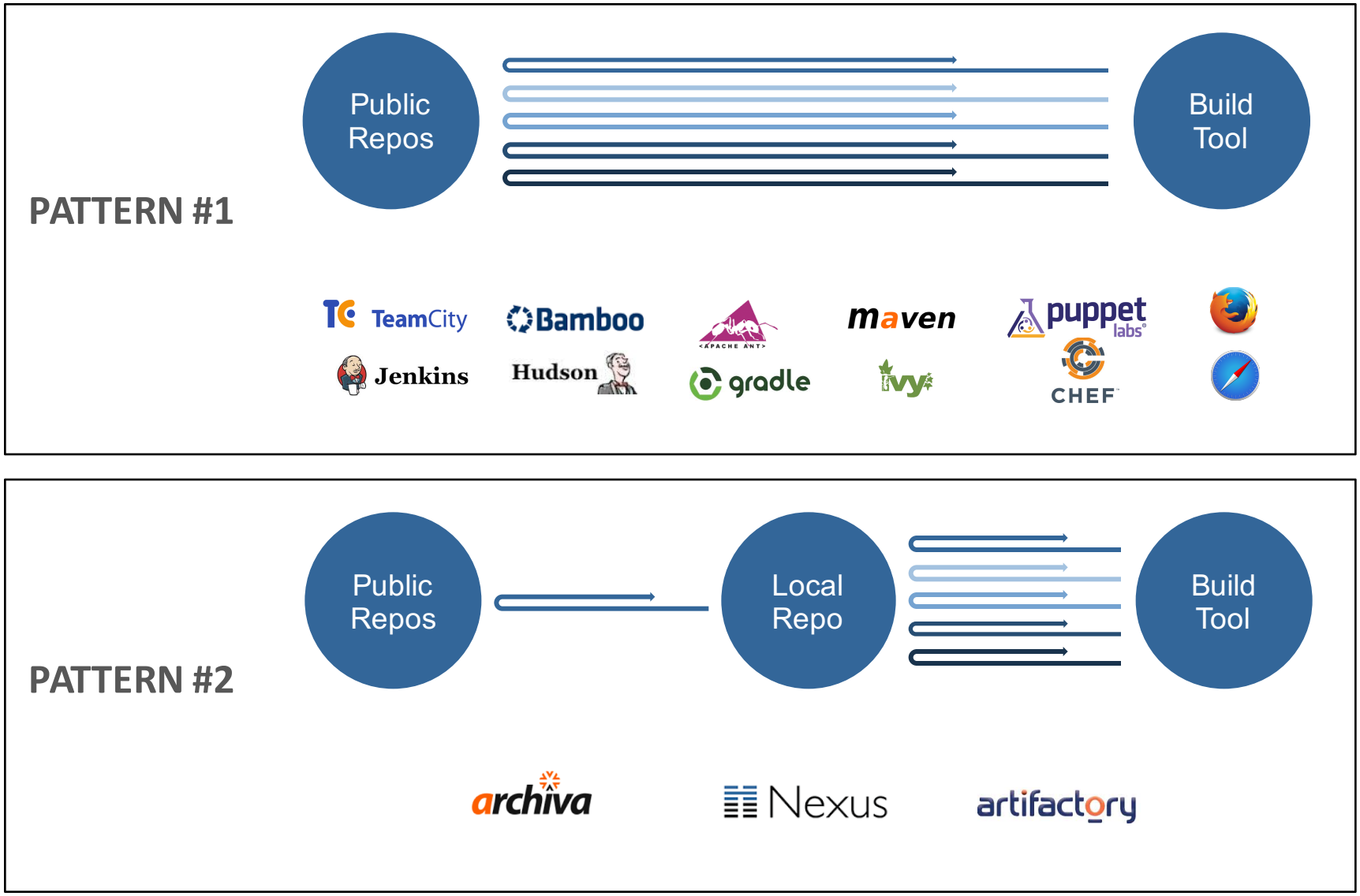
Unlike COTS, there is no clear, effective

COMMUNICATION

channel

11 MILLION OSS USERS

...but there can be.



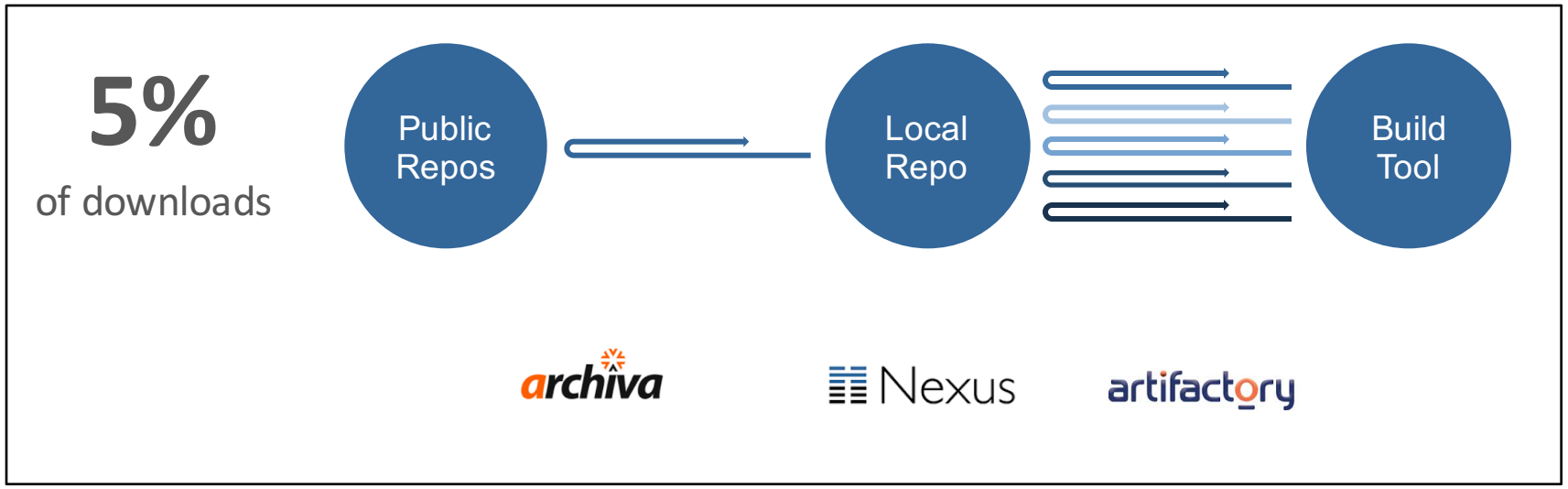
Source: 2015 State of the Software Supply Chain Report

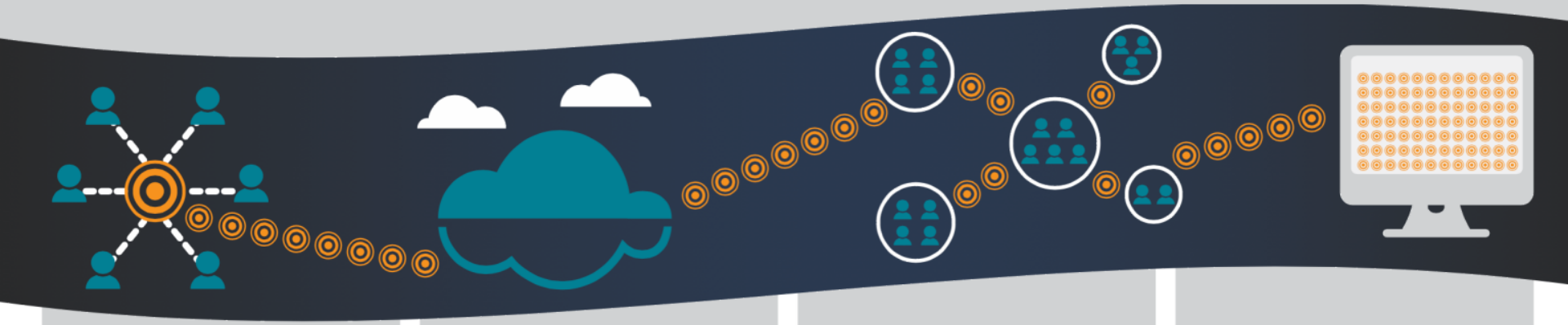
POLLING QUESTION

What percent of components are sourced from repository managers vs. other tools?

a. 25%
b. 55%
c. 95%


95%
of downloads
Public Repos
Build Tool
TeamCity
Bamboo
Jenkins
Hudson
gradle
maven
ivy
puppet labs
CHEF


5%
of downloads
Public Repos
Local Repo
Build Tool
archiva
Nexus
artifactory

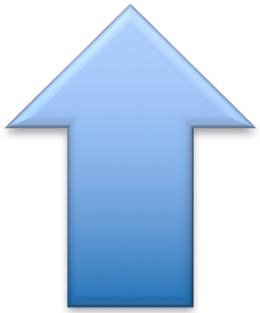


SUPPLIERS
Open Source Projects

WAREHOUSES
Component Repositories

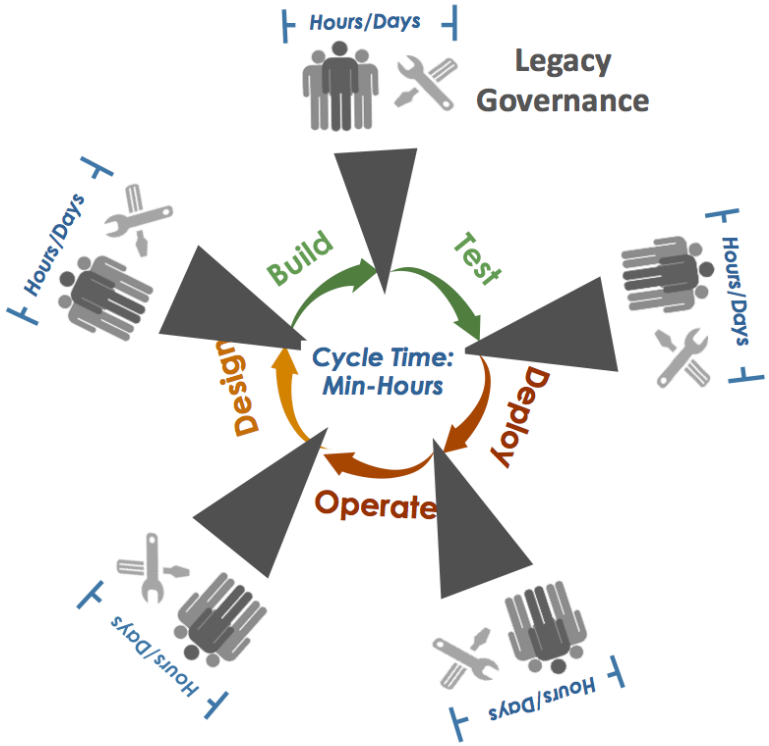
MANUFACTURERS
Software Development Teams

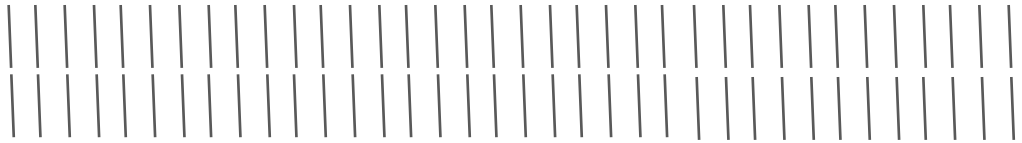
FINISHED GOODS
Software Applications



Oh, DevOps…

MANUFACTURERS
Software Development Teams





100-200

Cycle Time: Minutes-Hours

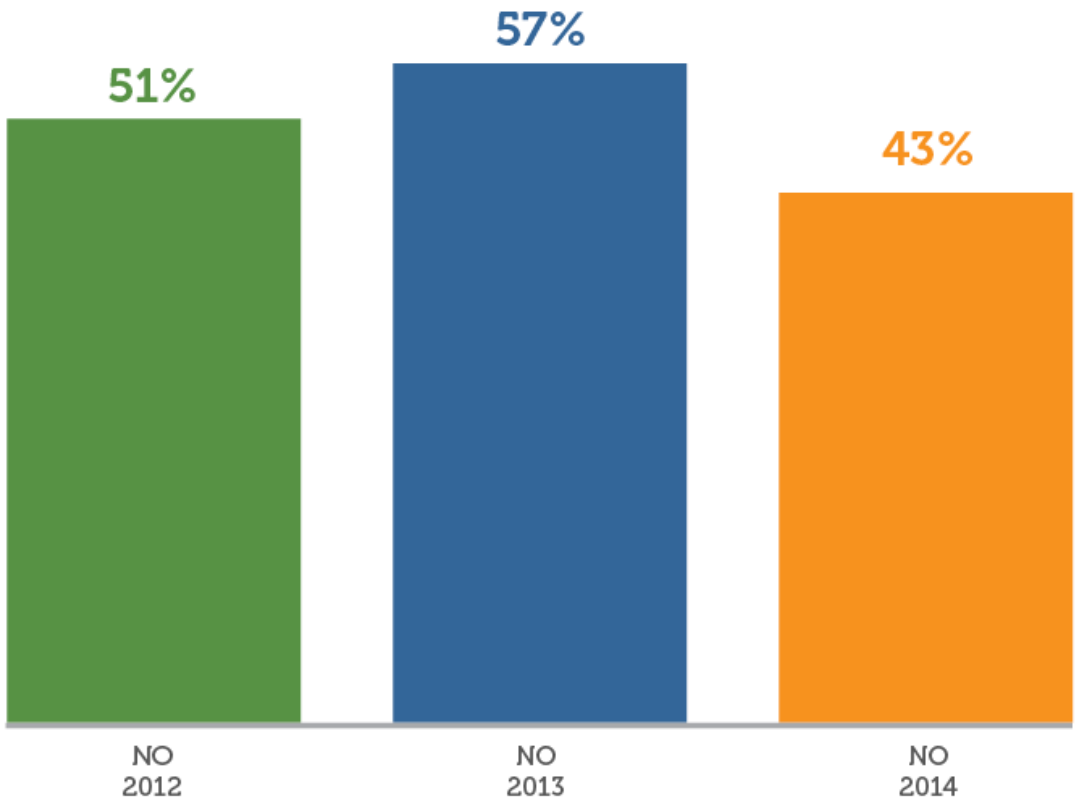
POLLING QUESTION

What percent of organizations do not have a policy governing quality and integrity of components?

a. 25%
b. 55%
c. 95%

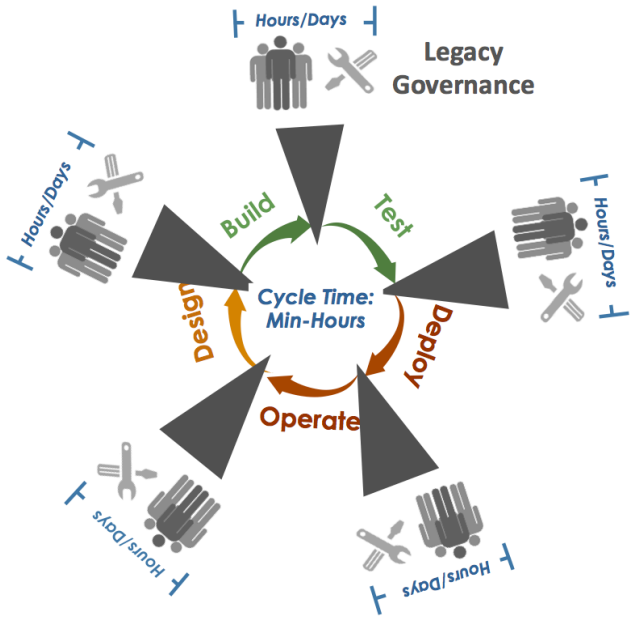
Half of organizations continue to run without an open source policy.

Q: Does your organization have an open source policy?



Source: 2012, 2013, 2014 Sonatype Open Source Development and Application Security Survey

MANUFACTURERS
Software Development Teams



If it does not fit, it does not get done.

Download Volumes of Old CVEs

Orders	Quality Control		
Average downloads	# with known vulnerabilities	% with known vulnerabilities	% known vulnerabilities (2013 or older)
240,757	15,337	7.5%	66.3%

Source: 2015 State of the Software Supply Chain Report

MANUFACTURERS
Software Development Teams

27

Outdated Versions Downloaded

Source: 2015 State of the Software Supply Chain Report

MANUFACTURERS
Software Development Teams

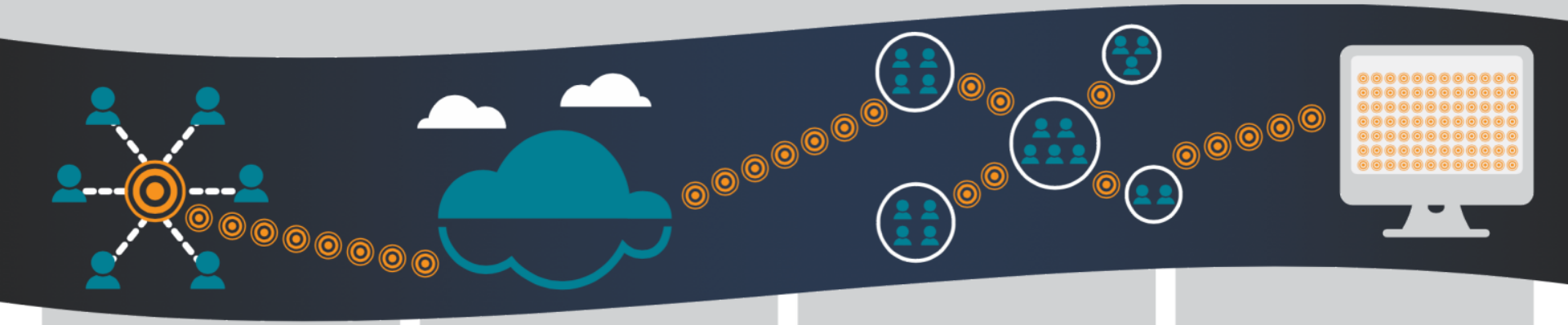
YOU WIN:

Taking meaningless work out of the system.

MANUFACTURERS
Software Development Teams

Google Search I'm Feeling Lucky

MANUFACTURERS
Software Development Teams

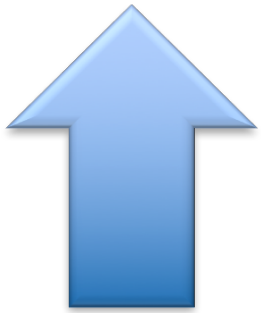


SUPPLIERS
Open Source Projects

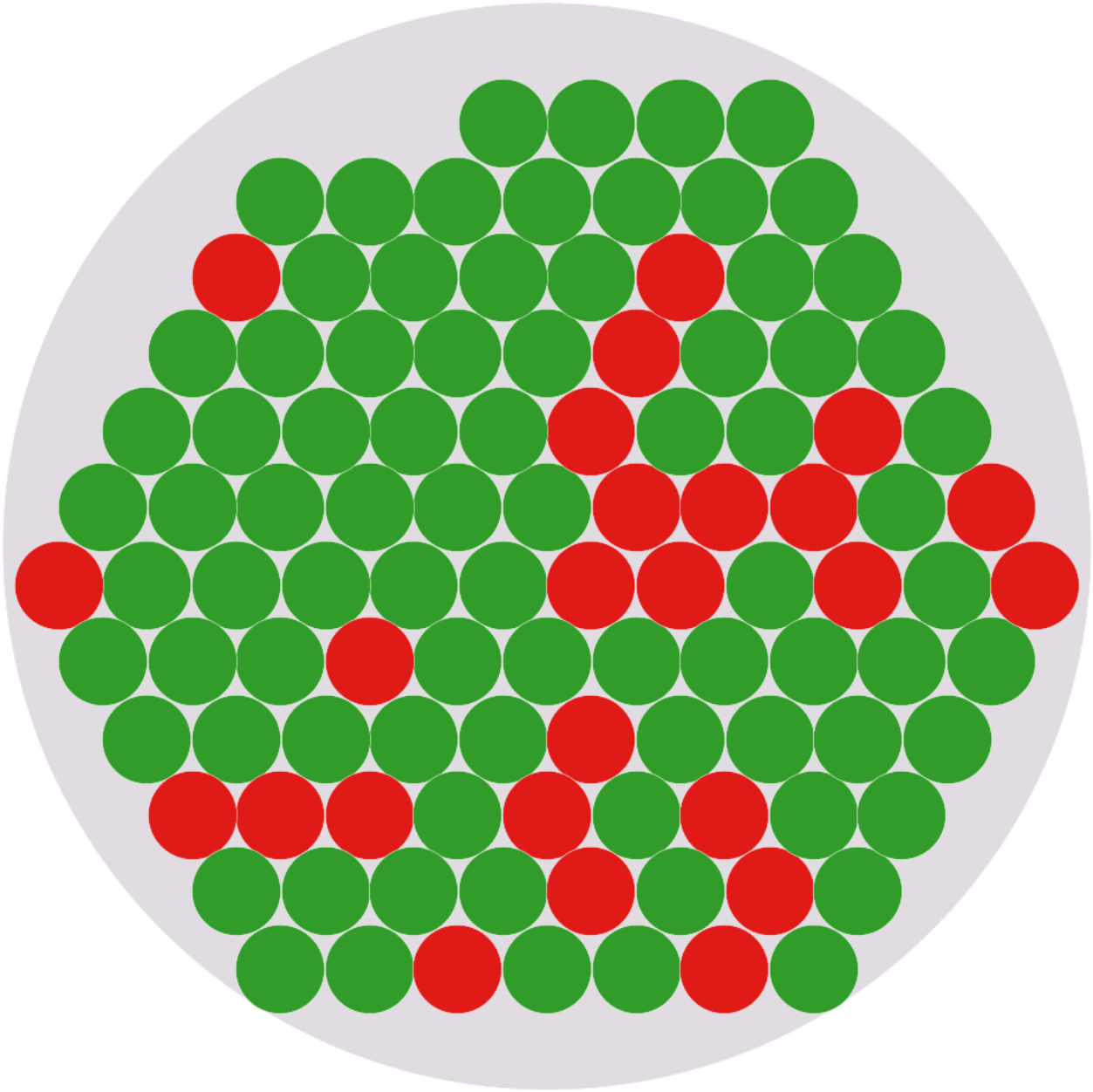
WAREHOUSES
Component Repositories

MANUFACTURERS
Software Development Teams

FINISHED GOODS
Software Applications



Analysis of 1,500+ applications…



software glitch

200,000 Jeeps recalled for ~~airbag issue~~ ^

By Peter Valdes-Dapena @peterdrives

COURTESY: FIAT CHRYSLER AUTOMOBILES

Fiat Chrysler Automobiles is recalling over 200,000 Jeep Grand Cherokees because side airbags could deploy unnecessarily when the SUV tilts to the side.

Fiat Chrysler Automobiles is recalling about 230,000 Jeep Grand Cherokees worldwide to fix a software problem that could cause the vehicles' airbags to deploy even when there's no real risk of a crash.

Most Popular


Judge throws out United Airlines lawsuit against 22-year-old


Tesla's new product is a battery for your home

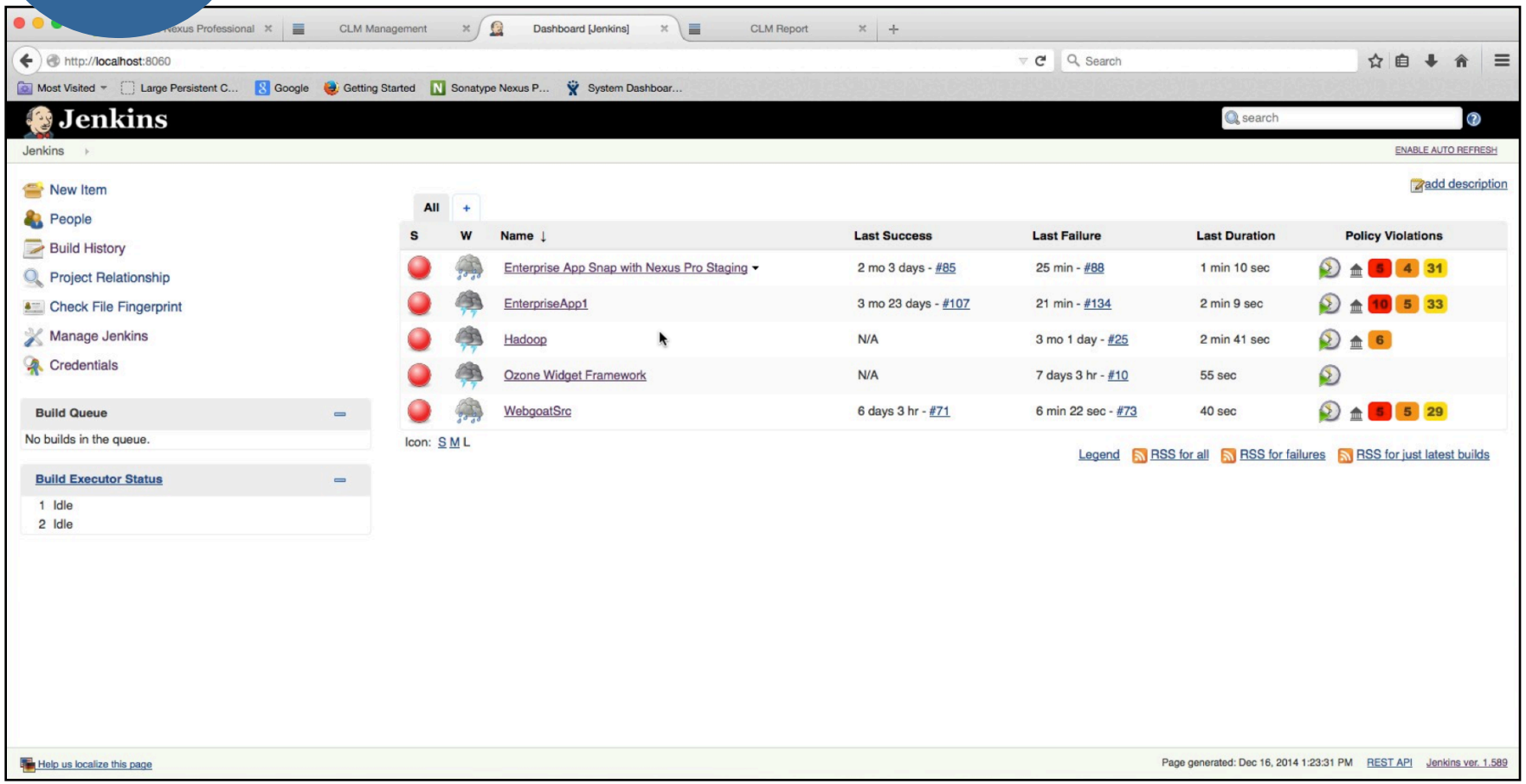

Floyd Mayweather: The star athlete no sponsor will touch

1 EMPOWER DEVELOPERS FROM THE START

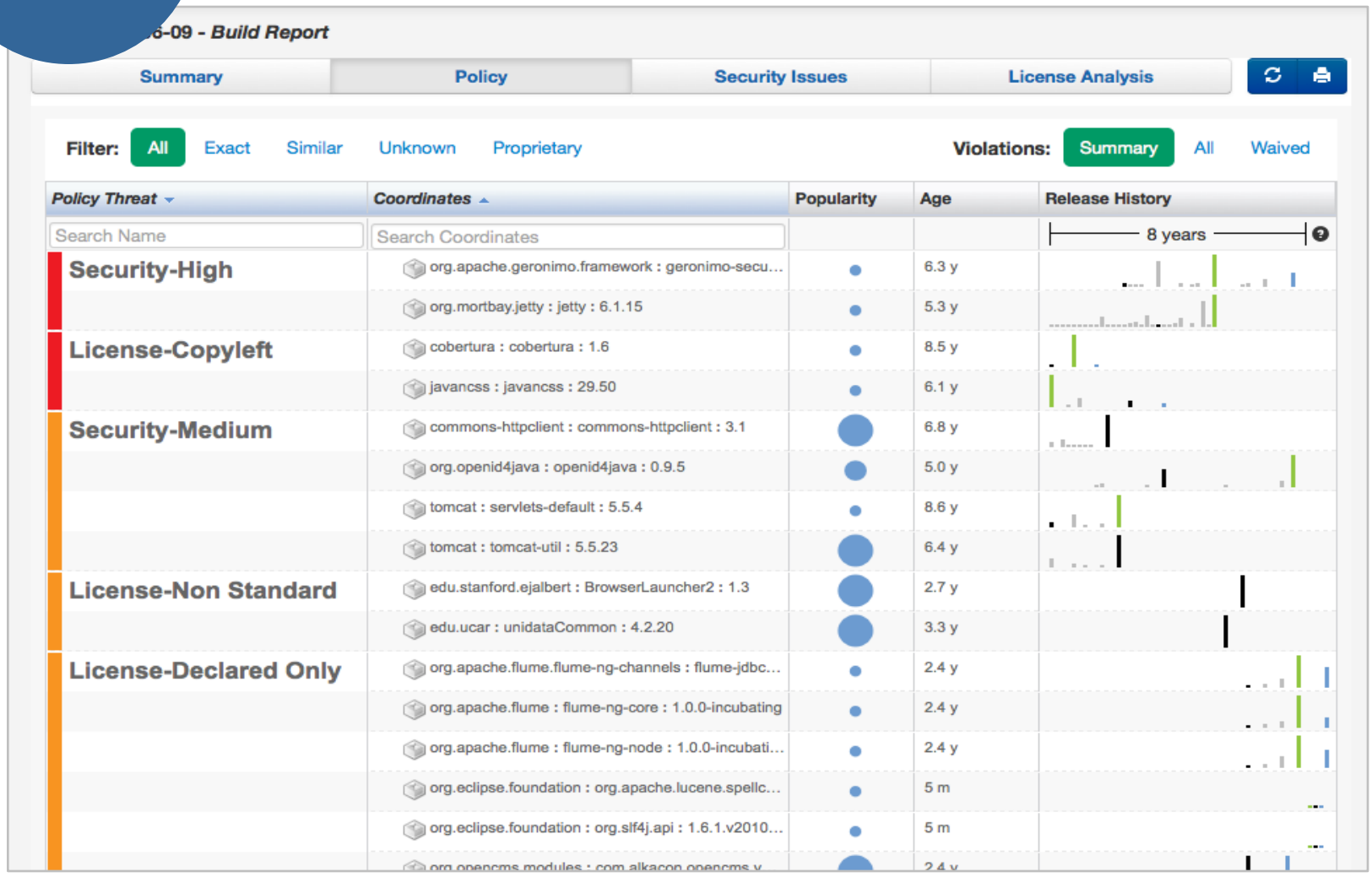
Group: **org.apache.struts**
Artifact: **struts2-core**
Version: **2.3.4**
Overridden License: **-**
Declared License: **Apache-2.0**
Observed License: **Apache-2.0**
Highest Policy Threat: **9** **within 2 policies**
Highest Security Threat: **10** **within 19 security issues**
Cataloged: **1 year ago**
Match State: **exact**

ZTTR (Zero Time to Remediation)

2 DESIGN A FRICTIONLESS APPROACH

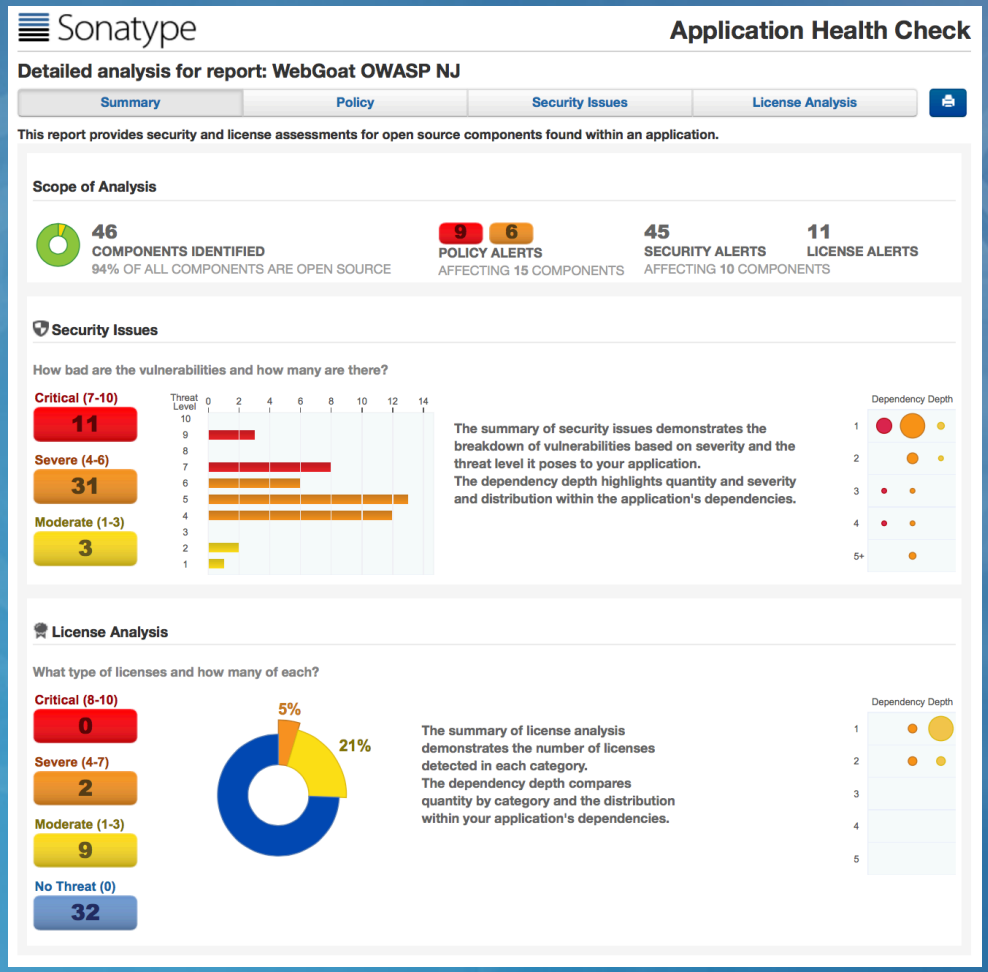


3 CREATE A SOFTWARE BILL OF MATERIALS



Your Bill of Materials:

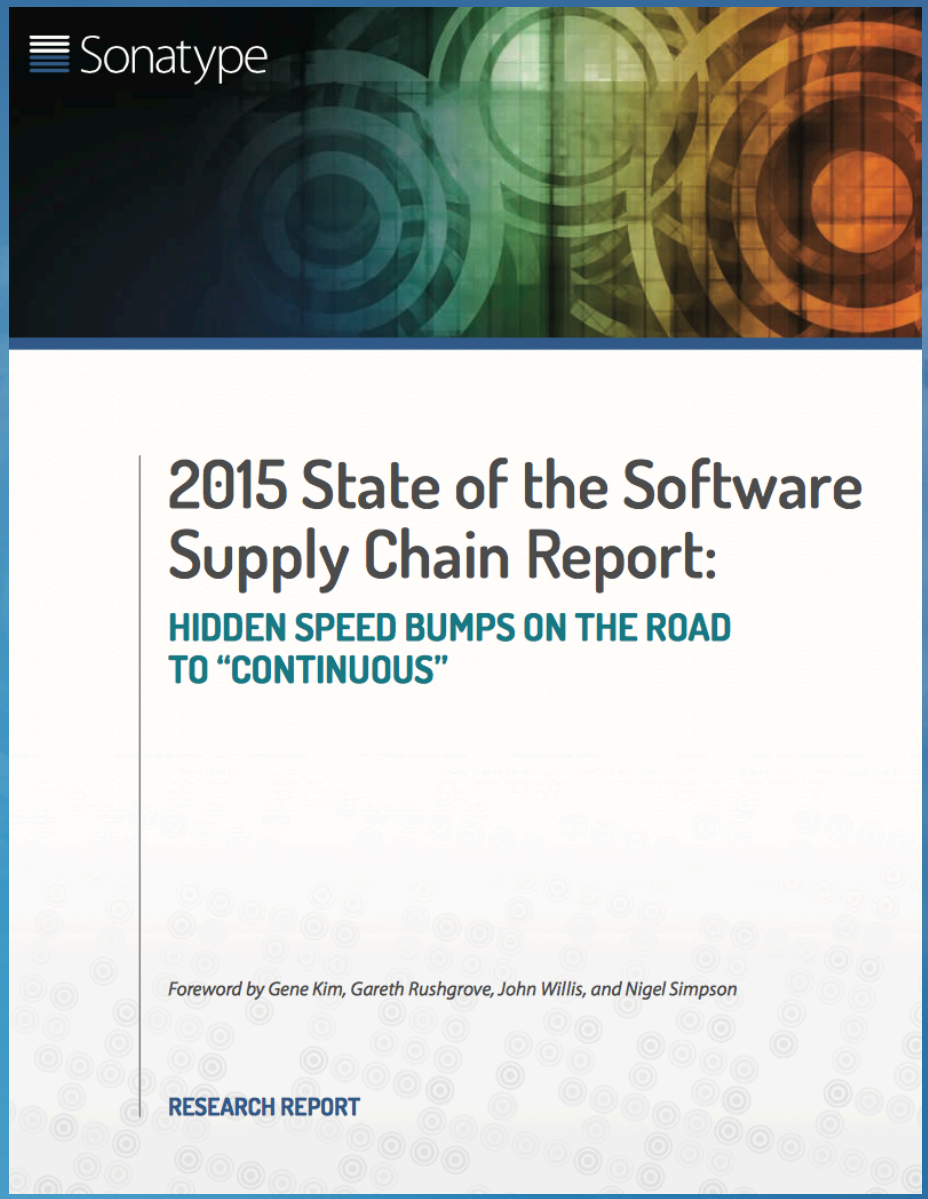
bit.ly/Sonatype_BOM



Sonatype

GET MY SLIDES NOW:

weeks@sonatype.com



Sonatype