



Tackling the Risks of Open Source Security

Elad Tzur

Channel Director EMEA & APAC at
WhiteSource



Case Study – Equifax

Data Breach – Sequence of Events

EQUIFAX

MARCH 7th:
Exploit code appear in the wild for a new vulnerability

MARCH 10th:
CVE-2017-5638 is published.
Fix out the same day

Patching window 2 months

Attack period

JULY 29th:
Breach is discovered by Equifax. Reports suggest unauthorized access started in May

SEPTEMBER 7th:
A new RCE vulnerability is announced and fixed.
CVE-2017-9805

MARCH

APRIL

MAY

JUNE

JULY

AUGUST

SEPTEMBER

Enough Time to Respond

- Time Equifax had to patch

About 8-9 Weeks

- Attack period

About 10 Weeks

- Time between detection and notice

About 6 Weeks



Incident Aftermath

- Equifax admitted the thieves stole **personal and sensitive data**
- The data taken affected as many as **143 million people**, roughly **half of US population**
- The breach is labelled as the **largest & worst corporate data breach in history**



Impact on Equifax

Equifax Breach: Two Executives Step Down as Investigation Continues

By NICOLE PERLROTH and CADE METZ SEPT. 14, 2017



FINANCE • EQUIFAX

Equifax Stock Has Plunged 18.4% Since It Revealed Massive Breach



BUSINESS DAY

Trying to Stem Fallout From Breach, Equifax Replaces C.E.O.

By RON LIEBER and STACY COWLEY SEPT. 26, 2017



- October 3 10 comments
Former Equifax CEO blames breach on a single person who failed to deploy patch
by Russell Brandom | @russellbrandom
The company is still investigating
- September 26
Equifax's CEO is stepping down in the wake of the massive data breach
by Colin Lecher | @colinlecher
- September 21 9 comments
Experian allows users to undo a credit freeze just by knowing a handful of breachable facts
by Ashley Carman | @ashleyrcarman
- September 20 20 comments
For weeks, Equifax customer service has been directing victims to a fake phishing site
by Dani Deahl and Ashley Carman
- September 19 13 comments
New evidence raises doubts about executives' handling of the Equifax breach
by Thuy Ong | @ThuyOng
A breach happened in March, months earlier than the company previously admitted to

Stock Still Didn't Rebound

AT CLOSE 4:02 PM EST 11/06/17

\$108.03 USD

Down 24.3%

Worth \$4.17B in Market Cap



Apache Struts Adoption Statistics

According to WhiteSource Research

**58% are using Struts
(any version)**

**20% are exposed to the 2
specific Equifax CVEs**

**Organizations on the
latest (patched) Struts version –
1.3%**



4 Things Every CISO Needs To Know About Open Source Security



01

Open Source Risk
Is On The Rise



02

OSS Security vs.
Proprietary Code
Security



03

Efficiency & Noise
Reduction



04

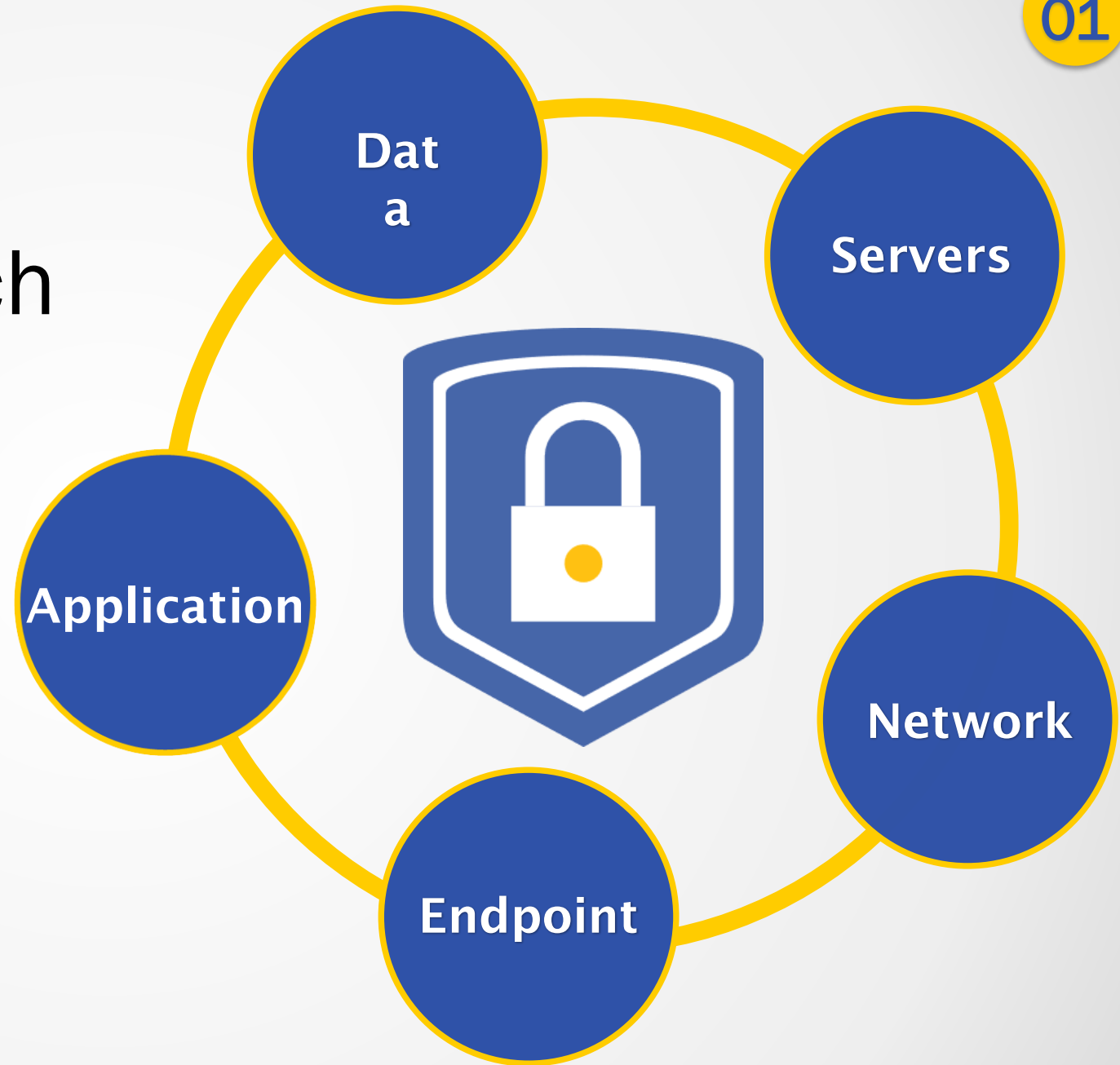
Shift Left & Delegate
Security
Responsibilities



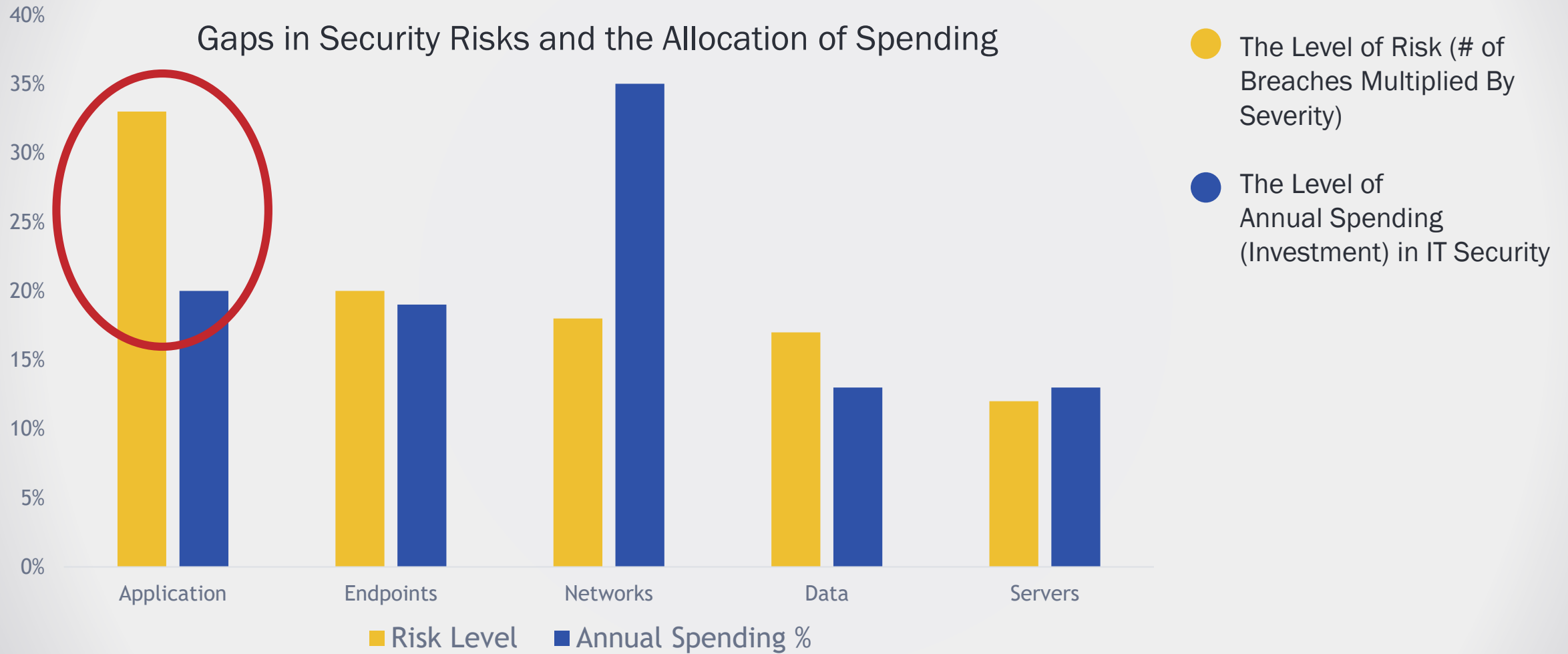
01

Open Source Risk
Is On The Rise

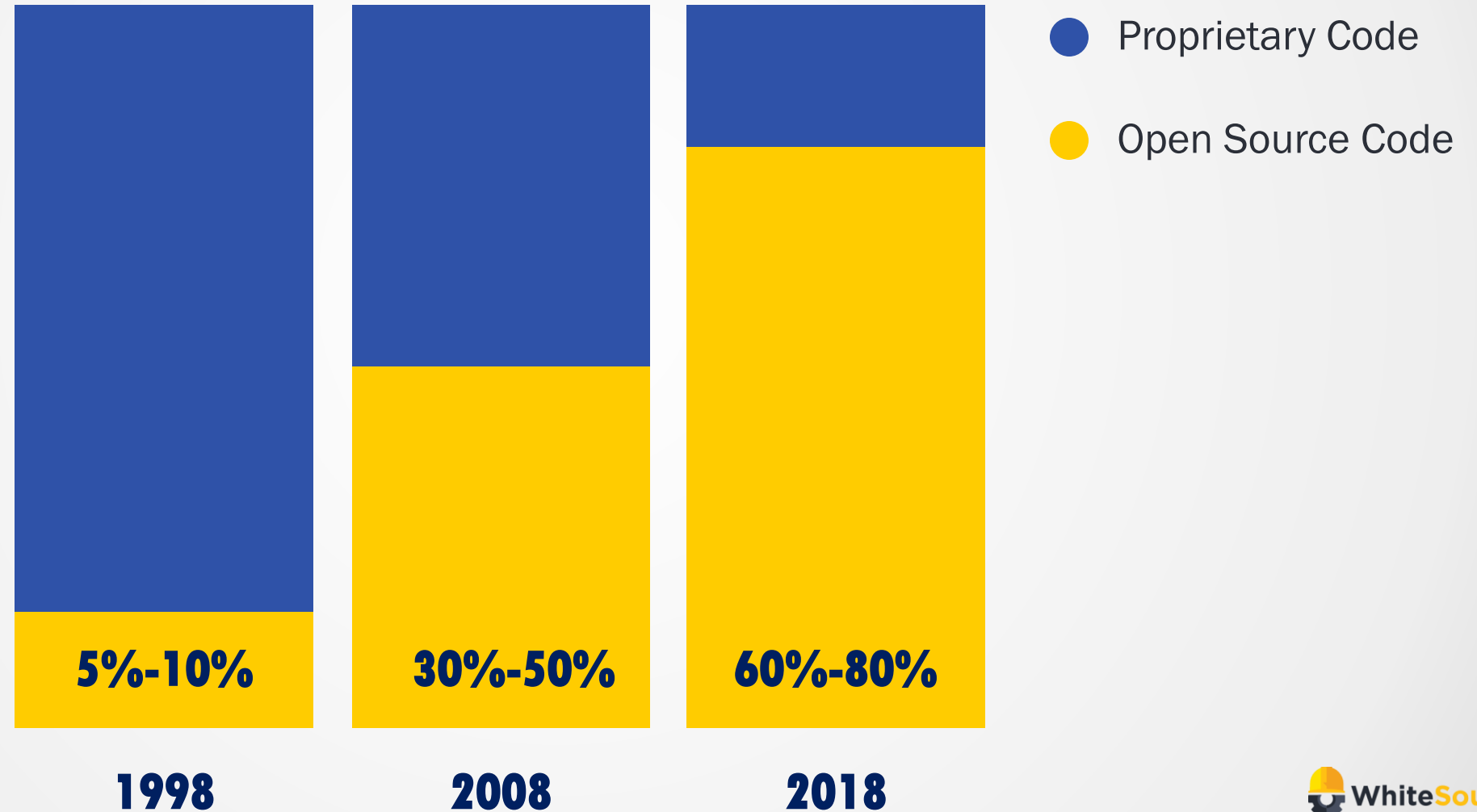
Security Spending
Is Expected To Reach
\$96 Billion
in 2018, But...



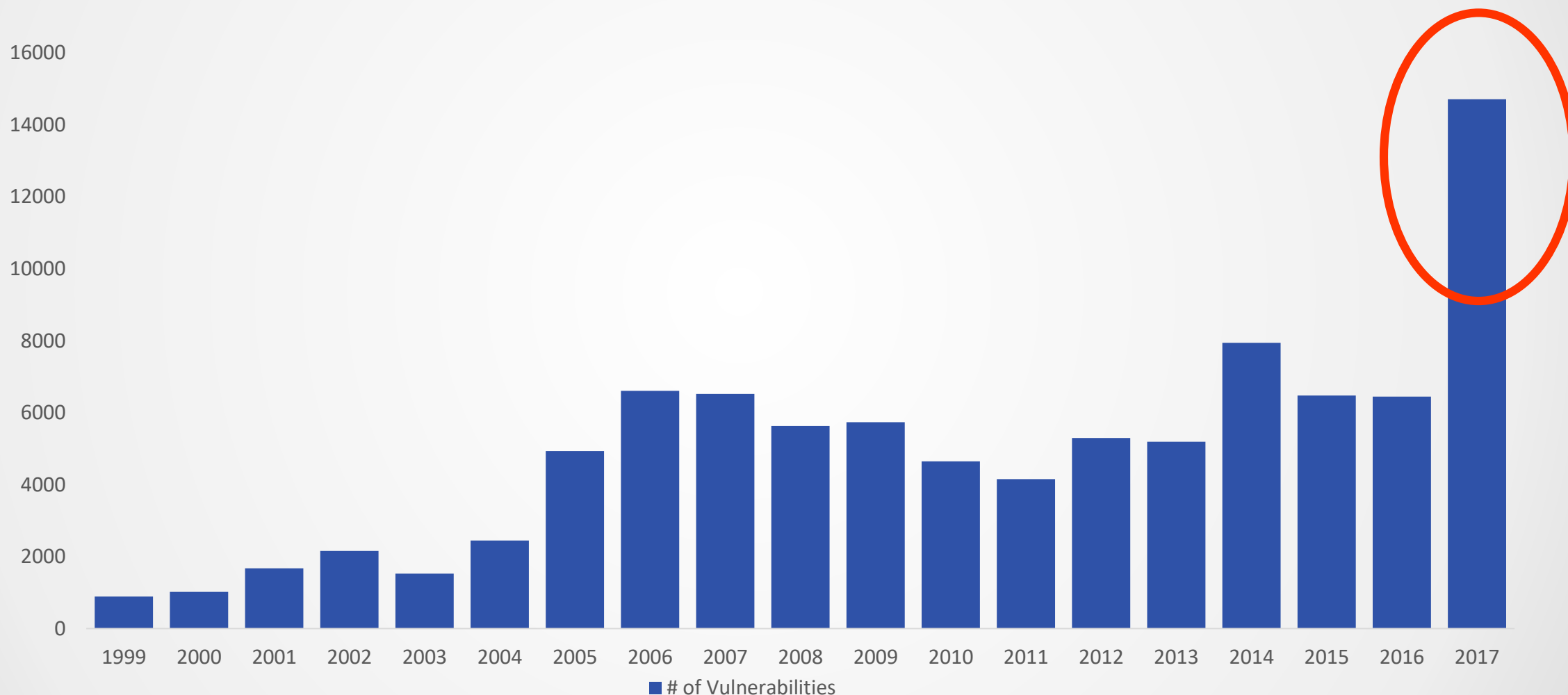
Are You Investing Enough in AppSec?



Open Source Components Account For 60%-80% Of The Average Software Product



Number Of New CVEs Discovered More Than **Doubled** YoY in 2017



Source: Common Vulnerabilities and Exposures



02

OSS Security vs.
Proprietary Code
Security

Open Source Security is a Different Game

Why is it so different than protecting your proprietary code?

PROPRIETARY VULNERABILITIES OPEN SOURCE VULNERABILITIES

Nature of Findings

Potential or suspected vulnerabilities (SAST & DAST)

Known & validated vulnerabilities (number of CVEs more than doubled in 2017)

What Do Hackers Know?

No public information available

All information is **publicly available**

How to Fix?

Need to analyze and come up with a fix

Fix suggestions are available (**87% of OSS vulnerabilities have a fix**)

When to Scan?

Typically post coding

Continuous monitoring (incl. post release)



03

Efficiency & Noise
Reduction

Effective vs Ineffective Open Source Code

Ineffective

70%

On average, **70%*** of reported security vulnerabilities in open source libraries are not referenced by the developers' code.

Effective

30%



04

Shift Left & Delegate Security Responsibilities

Automate Security Tools To Improve Coverage While Reducing Friction

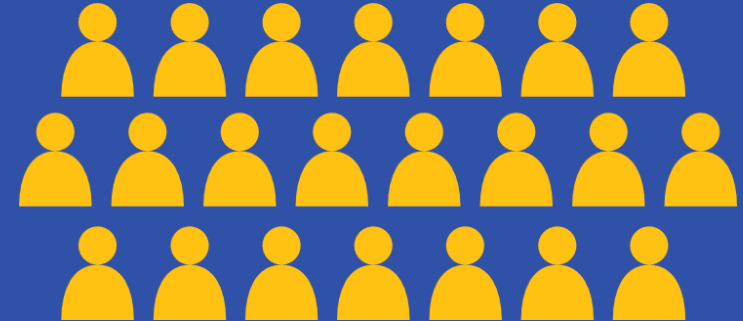
04



Security



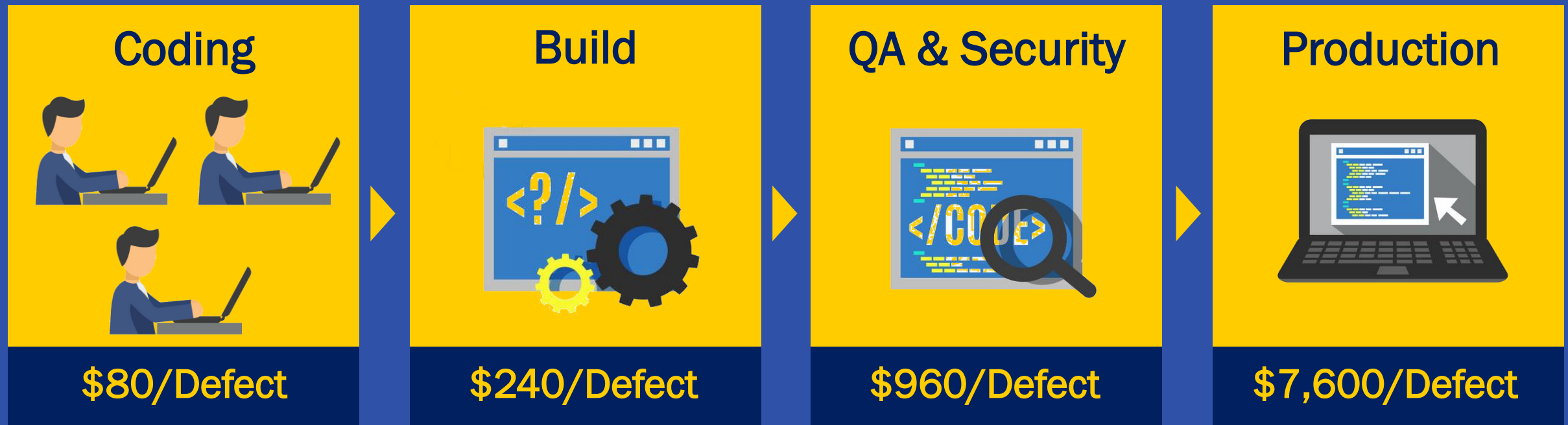
DevOps



Developers

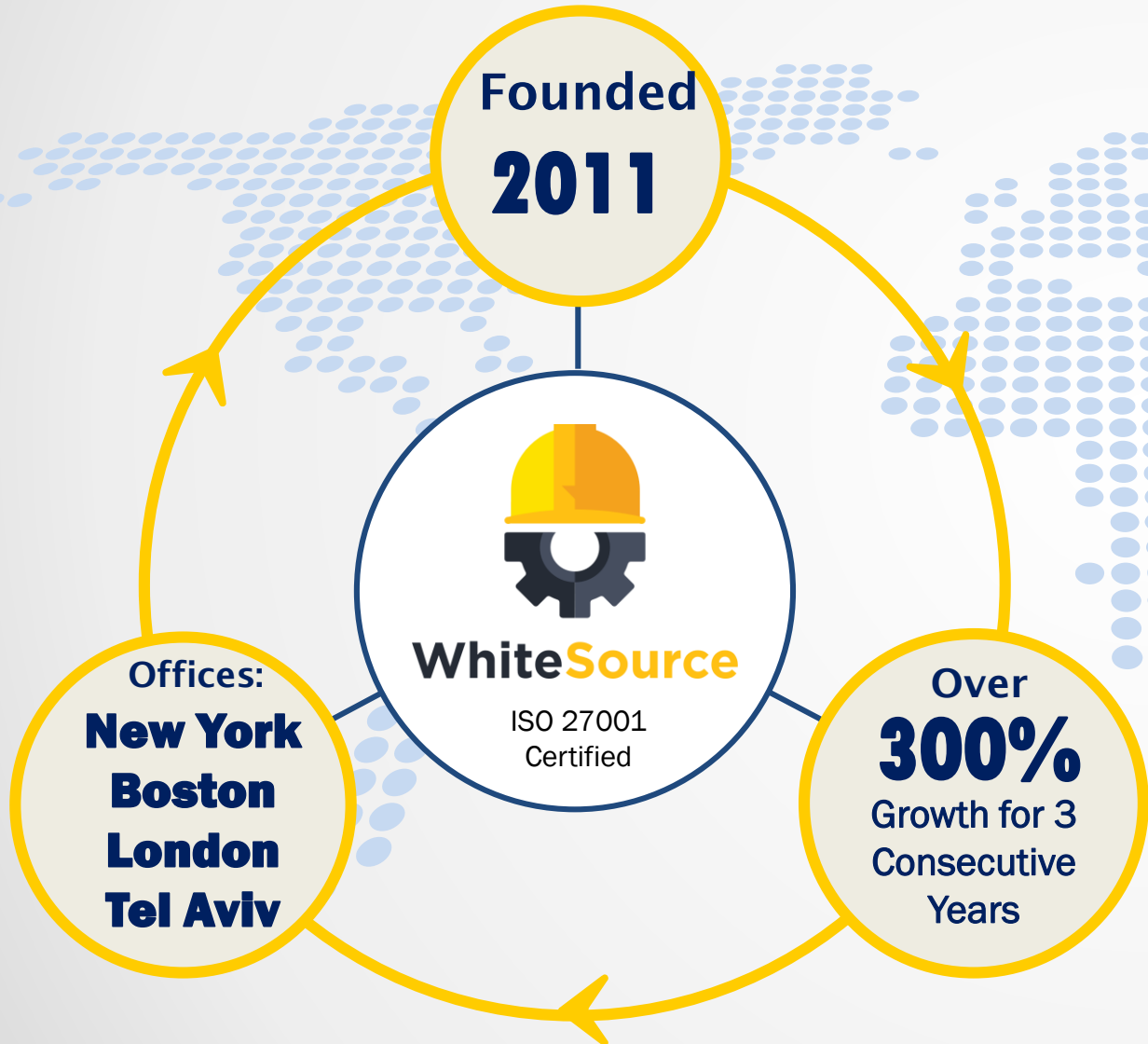
Detect Issues As Early As Possible

The cost of fixing security and quality issues is rising significantly, as the development cycle advances.



Cost of fixing issues reduced by 90% when detected in the build vs post release

WhiteSource | At a Glance



Over

400

Customers Worldwide

3 OEMs



IBM Security



CHECKMARX



aqua

WhiteSource Software

FORRESTER®

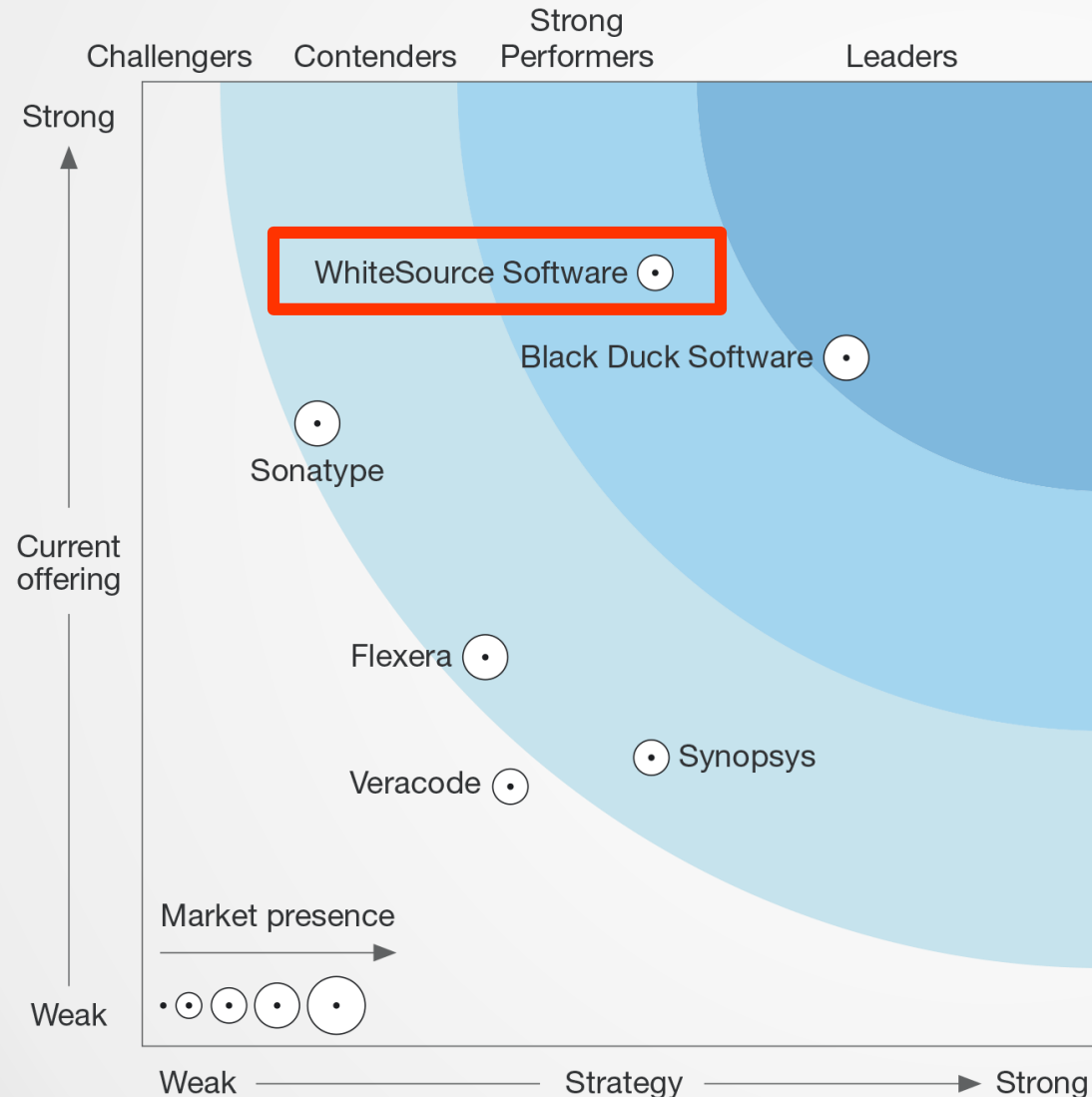
Scores Strongest Current Offering
in Forrester's Wave Report



Microsoft

Portfolio Company

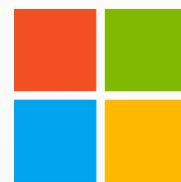
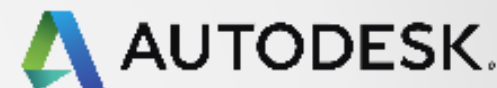
WhiteSource Scores Strongest Offering by Forrester®



“WhiteSource Software offers strong support for proactive vulnerability management, policy management and SDLC integration”

The Forrester Wave™: Software Composition Analysis (SCA) Q1 2017

Some of Our Customers



Microsoft



Summary – Open Source Security

Reality

CVE-2017-5638 is just one example.
Thousands of vulnerabilities found in OSS
yearly

Problem

OSS consumers i.e. developers or app
security personnel are **slow to react**

Good News

The OSS community is great at identifying
security issues & patching quickly – **just like**
in the Equifax case

Solution

Must be **combination of technology and**
mindset shift

Q&A Session



THANK YOU

