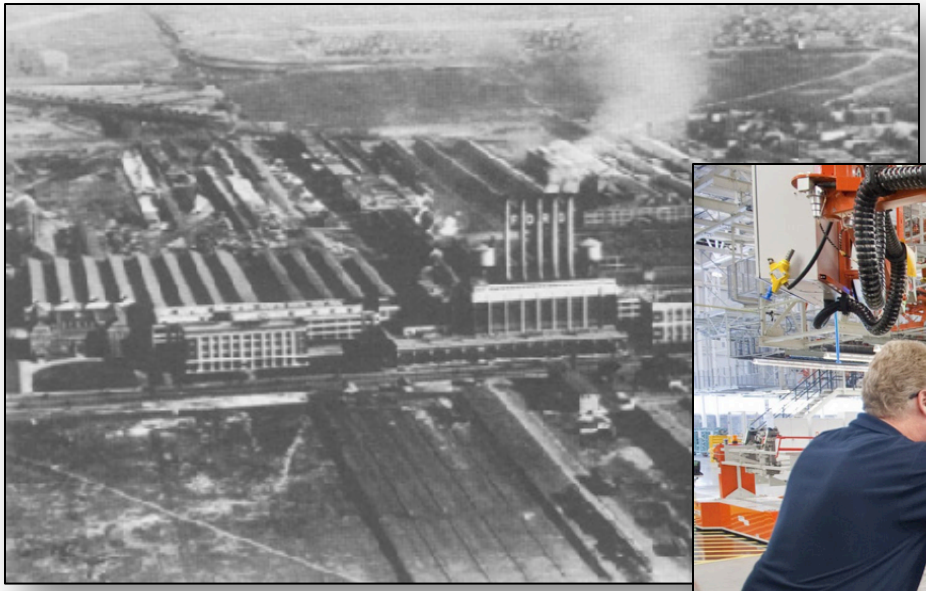
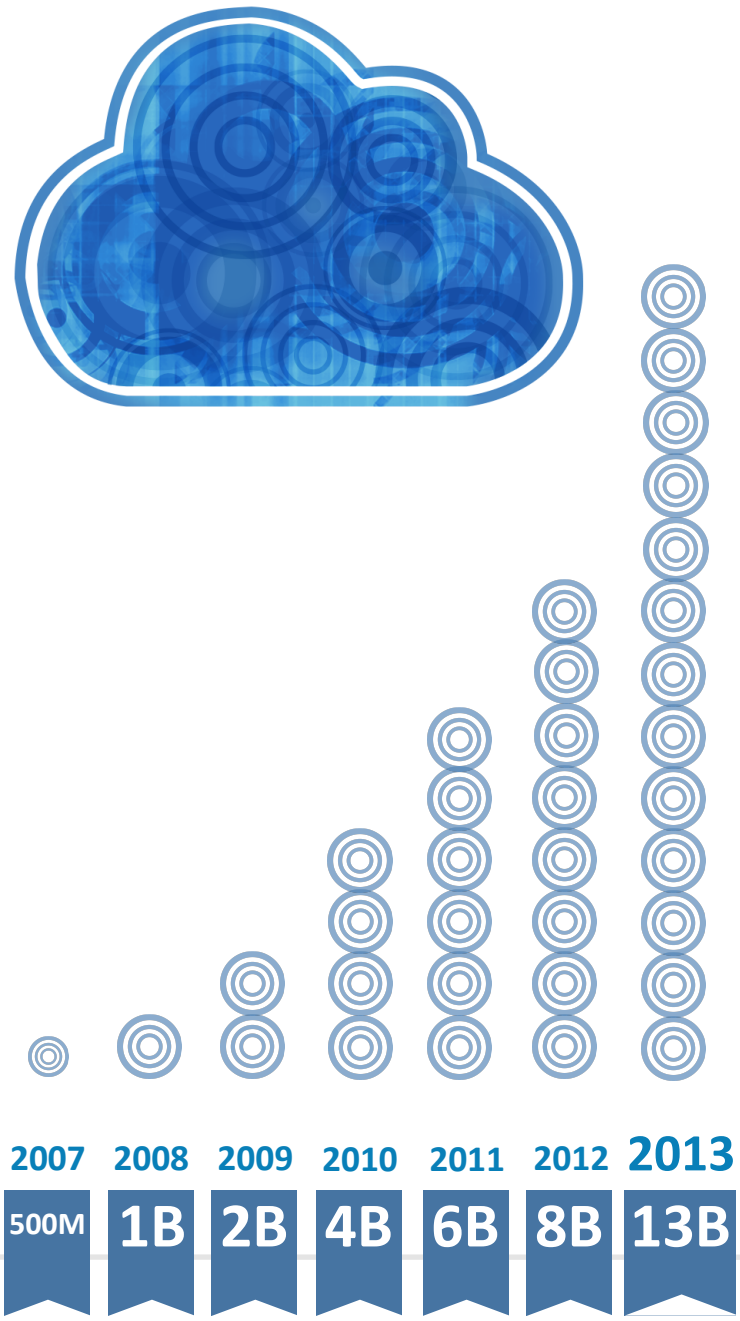
Open Source components fuel agile development

Supply chain solutions for modern development

Brian Fox @brian_fox

INDUSTRIAL EVOLUTION





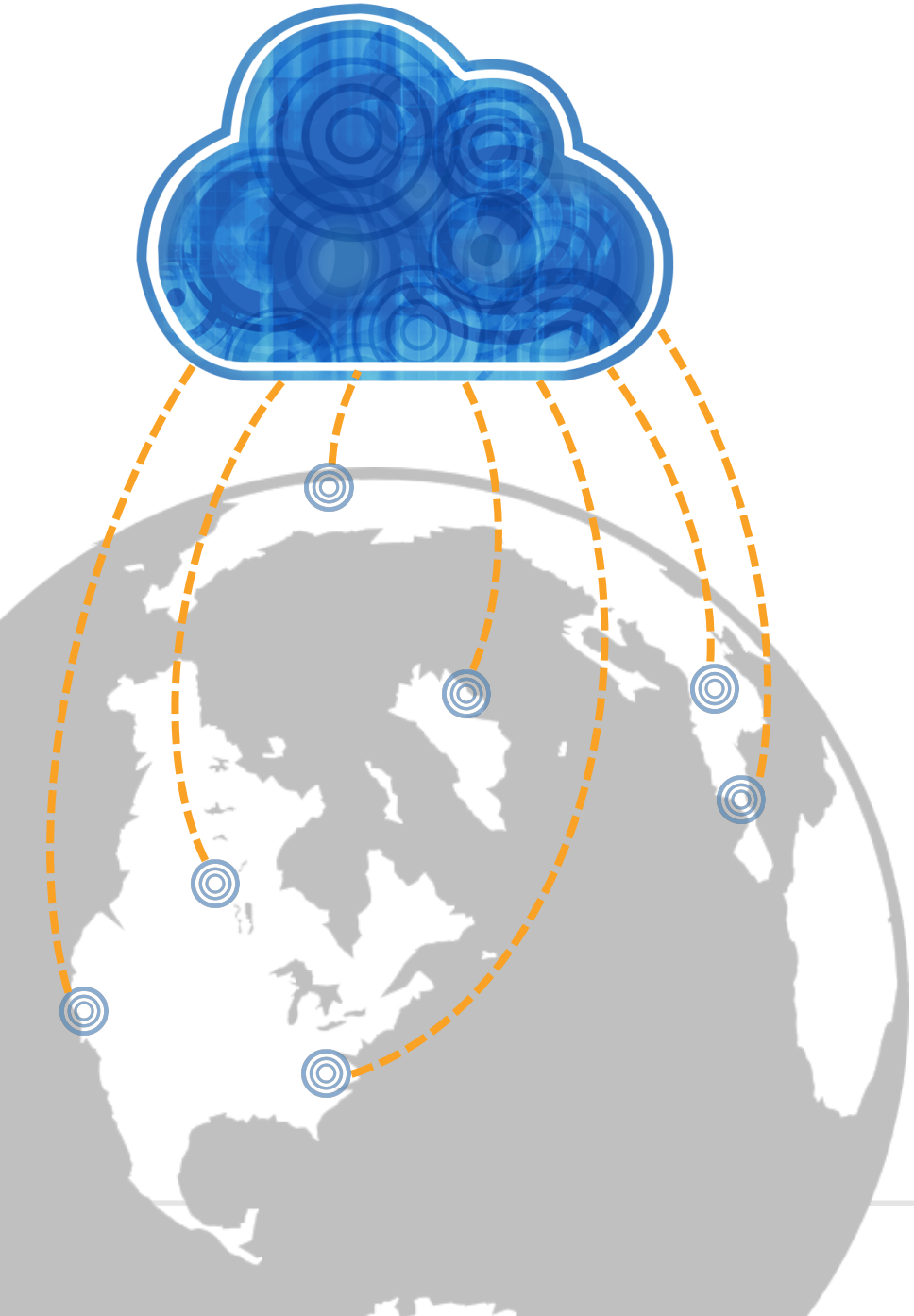
Open source usage is

EXPLODING

Yesterday's source code are today's

COMPONENTS

Sonatype

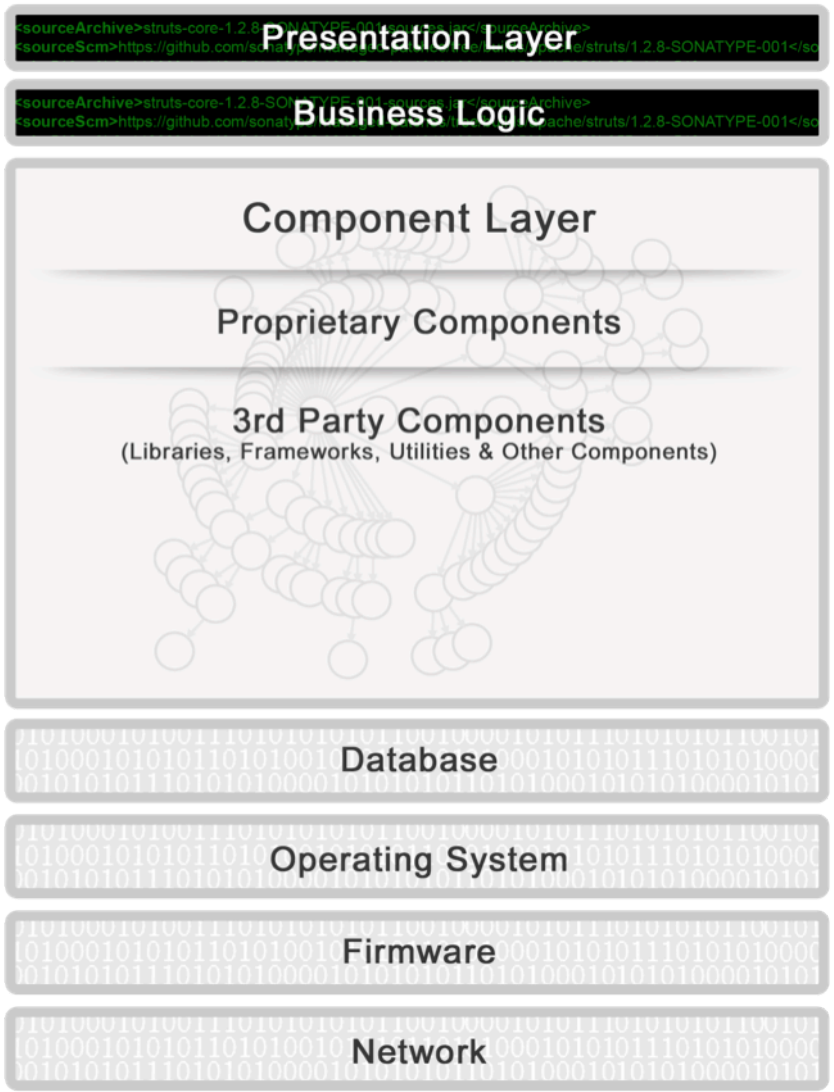


APPLICATIONS

are assembled using
third party “components,”
most of which are open source

In fact, **90%**
of a typical application
is open source

Sonatype

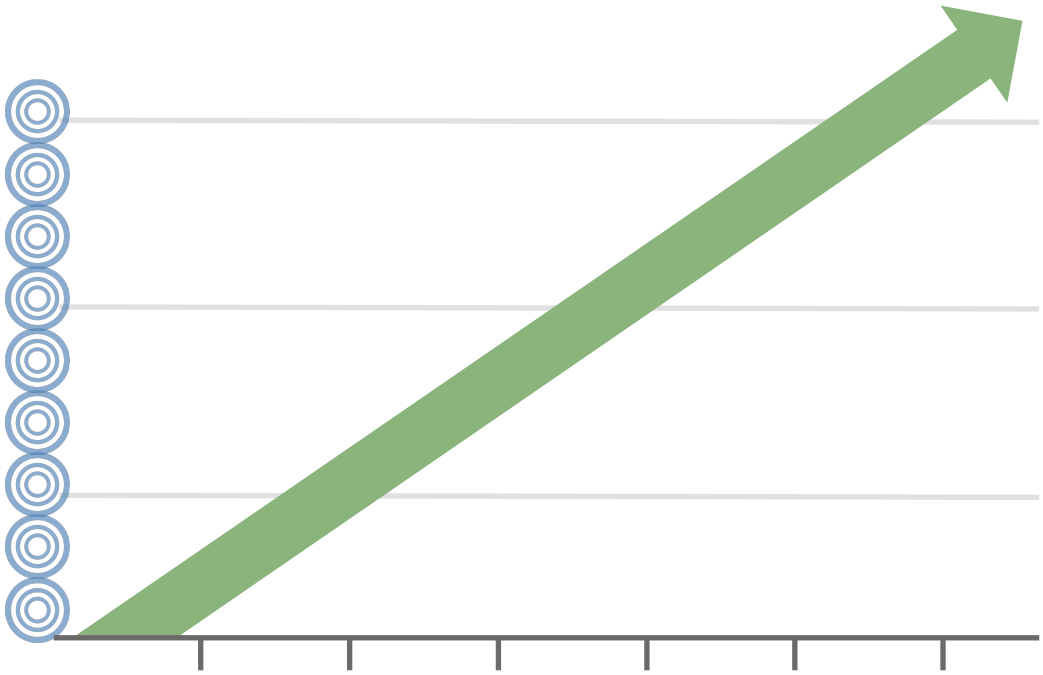

Presentation Layer
Business Logic
Component Layer
Proprietary Components
3rd Party Components
(Libraries, Frameworks, Utilities & Other Components)
Database
Operating System
Firmware
Network

OPEN SOURCE:

QUALITY

INNOVATION

EFFICIENCY



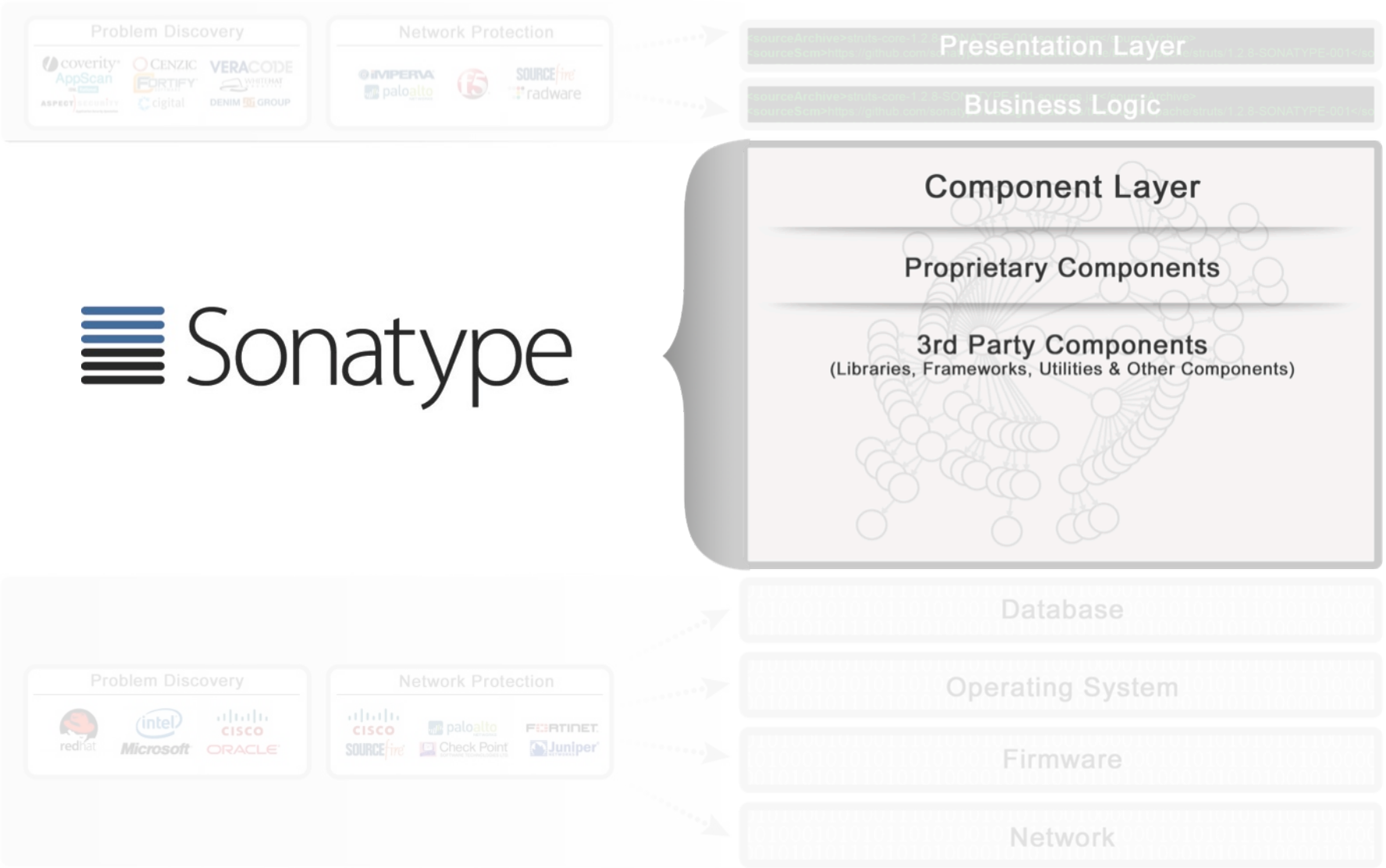
Modern software development

HAS CHANGED

Our process

HASN'T CHANGED ENOUGH

Sonatype



Sonatype

Sonatype

Spending and risk are

OUT OF SYNC

spending

People Security ~$4B

Data Security ~$5B

Component Security ~$0.4B

Host ~$10B

Network Infrastructure ~$20B

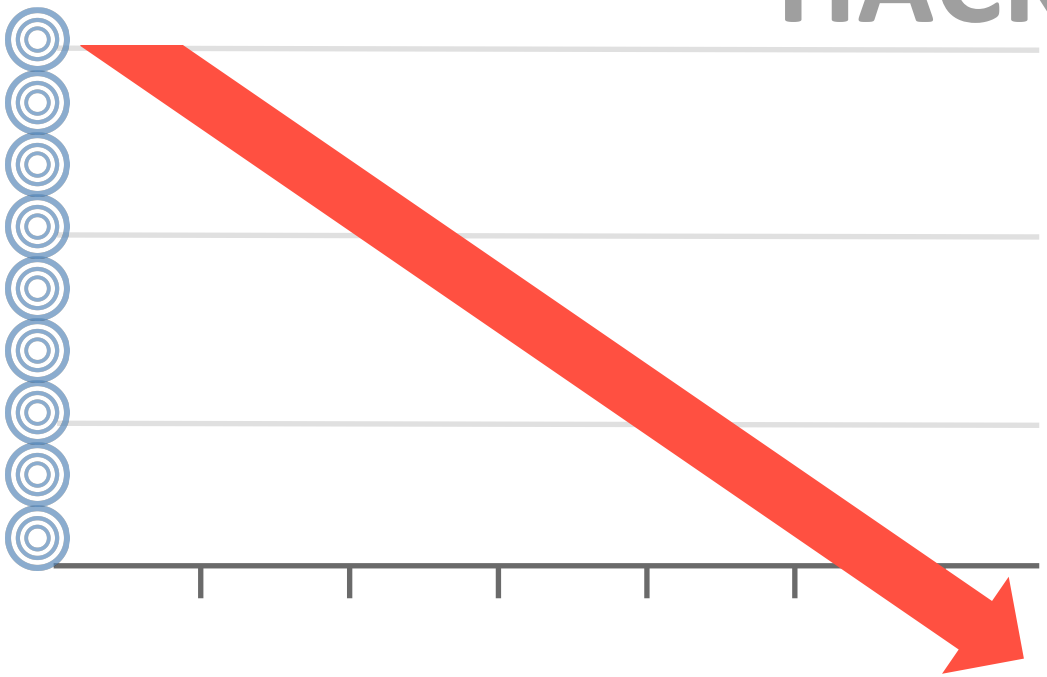
attack risk

Sonatype

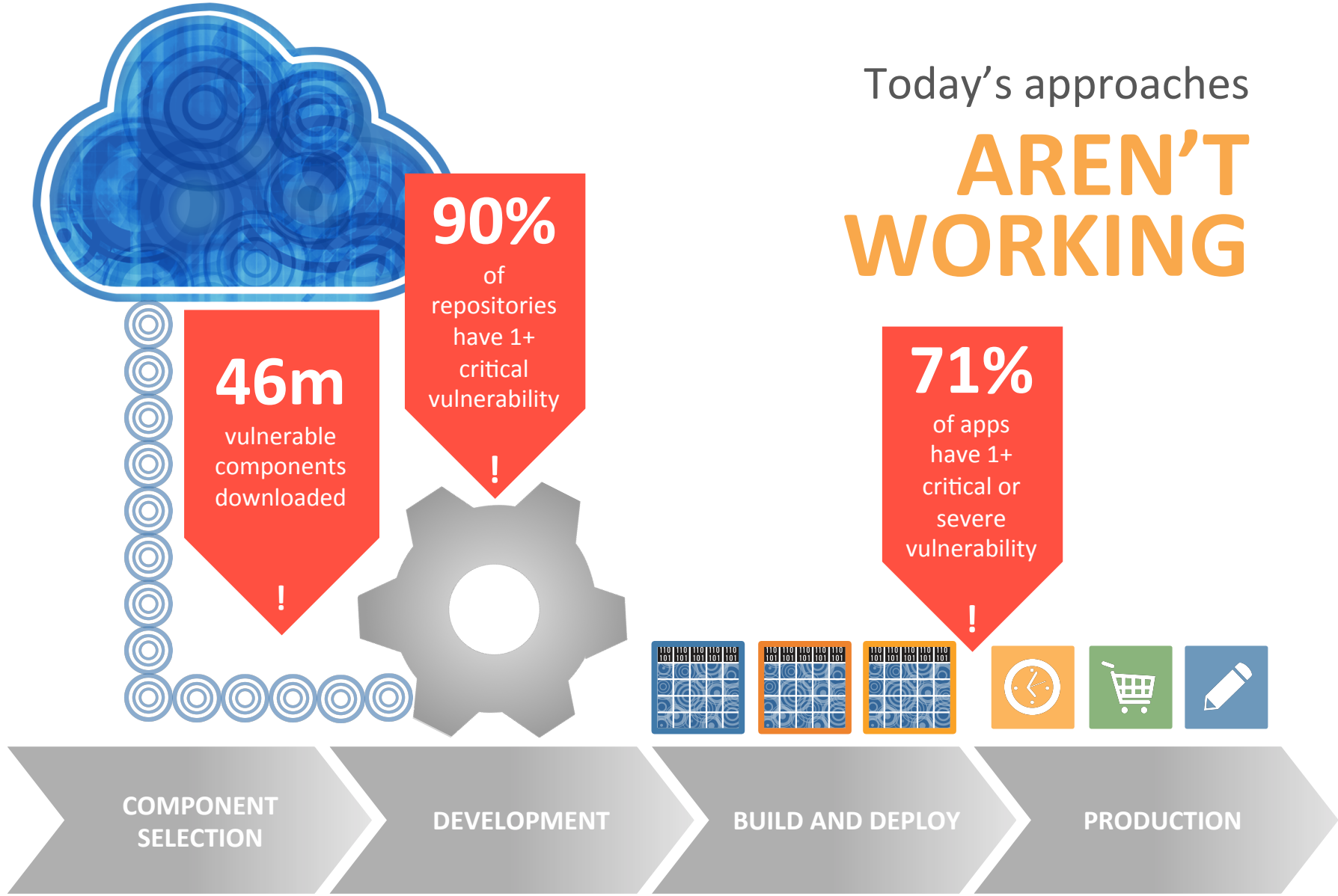
NO CONTROLS.

OPEN ACCESS.

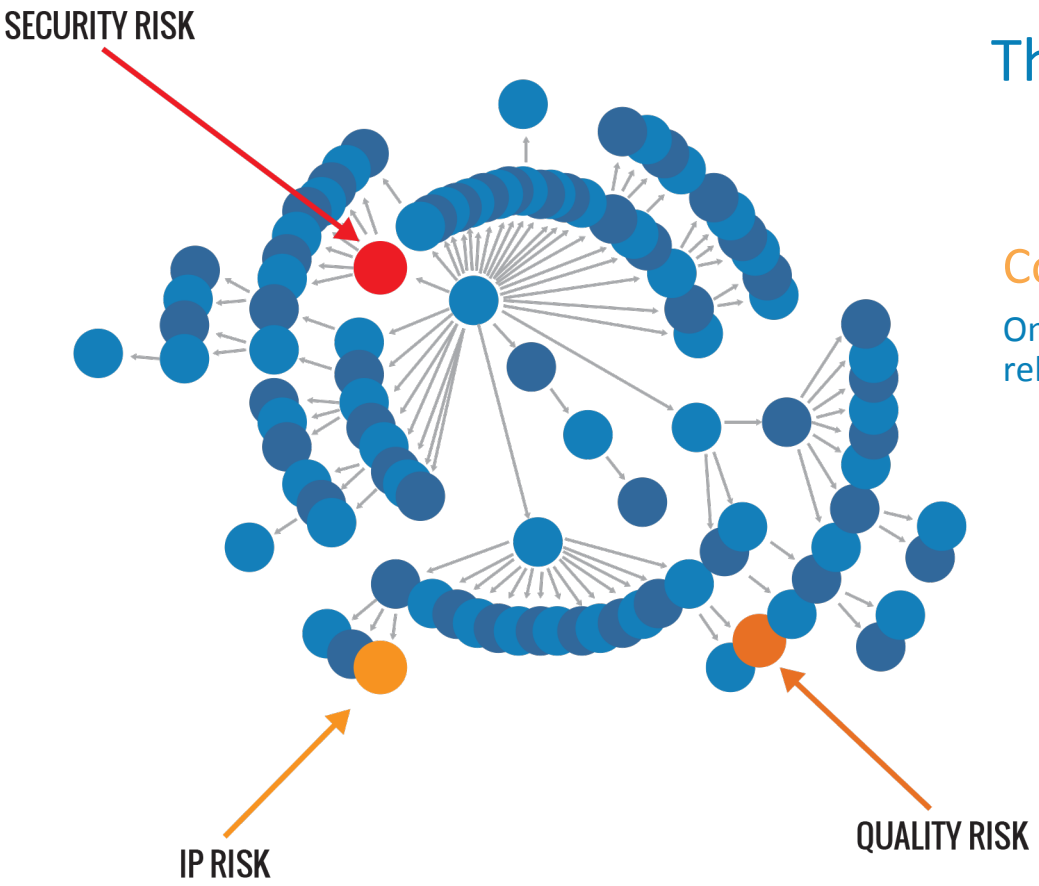
HACKER TARGETS.



Sonatype


Today's approaches
AREN'T WORKING
90%
of repositories have 1+ critical vulnerability
!
46m
vulnerable components downloaded
!
71%
of apps have 1+ critical or severe vulnerability
!
COMPONENT SELECTION
DEVELOPMENT
BUILD AND DEPLOY
PRODUCTION
Sonatype

WHY?



The problem is too complex to manage manually.

Complexity

One component may rely on 100s of others

Diversity

- 40,000 Projects
- 200M Classes
- 400K Components

Volume

Typical enterprise consumes 1,000s of components monthly

Change

Typical component is updated 4X per year

A MASSIVE SUPPLY CHAIN PROBLEM

No Visibility

No visibility to what components are used, where they are used and where there is risk

No Control

No way to govern/enforce component usage. Policies are not integrated with development .

No Fix

No efficient way to fix existing flaws.

We are not the first

INDUSTRY

to face this

CHALLENGE

Sonatype

When software was first being written,
finding exploitable code was like

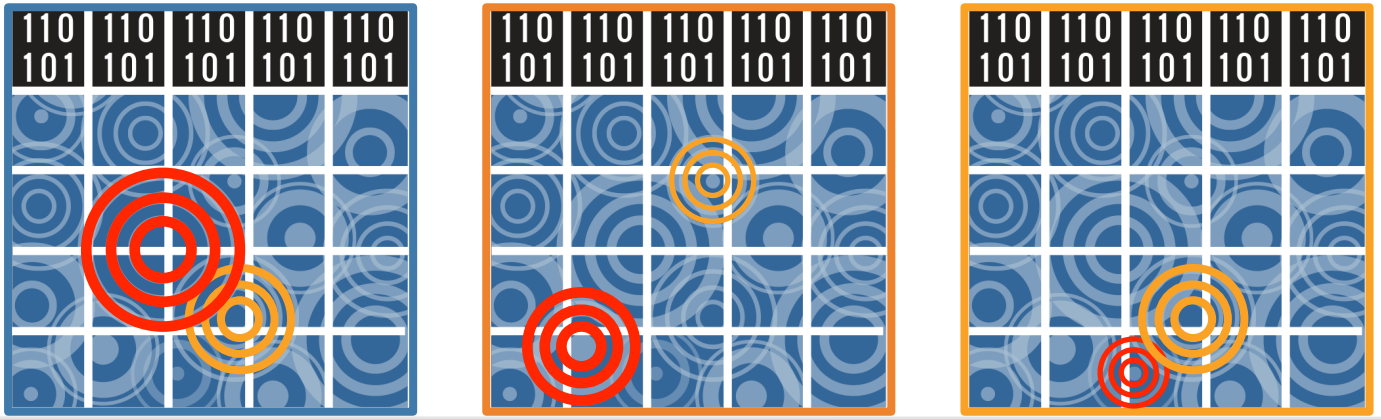
LOOKING

for a needle in a

HAYSTACK

Now that software is

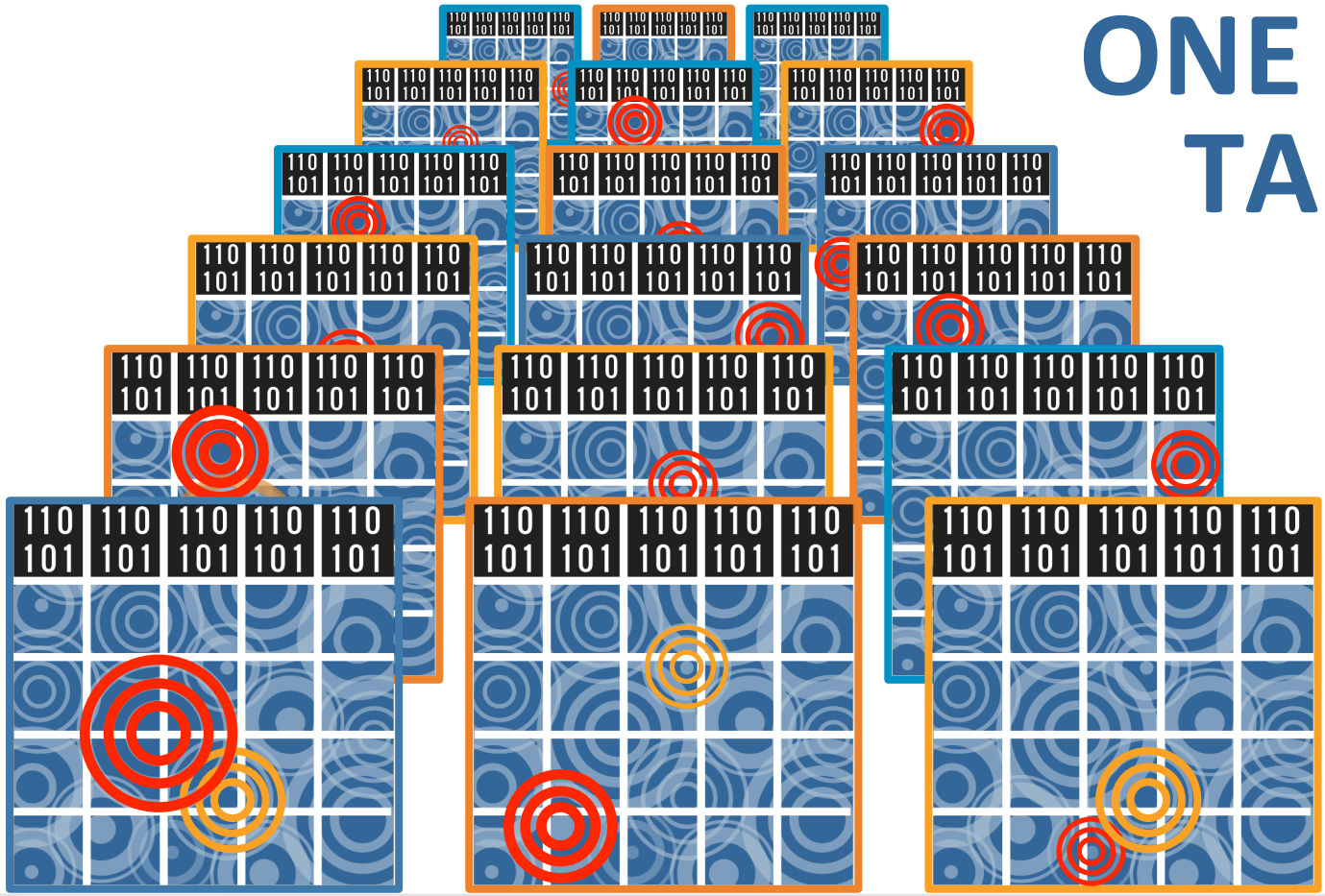
ASSEMBLED…



Sonatype

One risky component,
multiplied thousands of times:

ONE EASY TARGET



Sonatype

FOR EXAMPLE: CVE-2013-2251

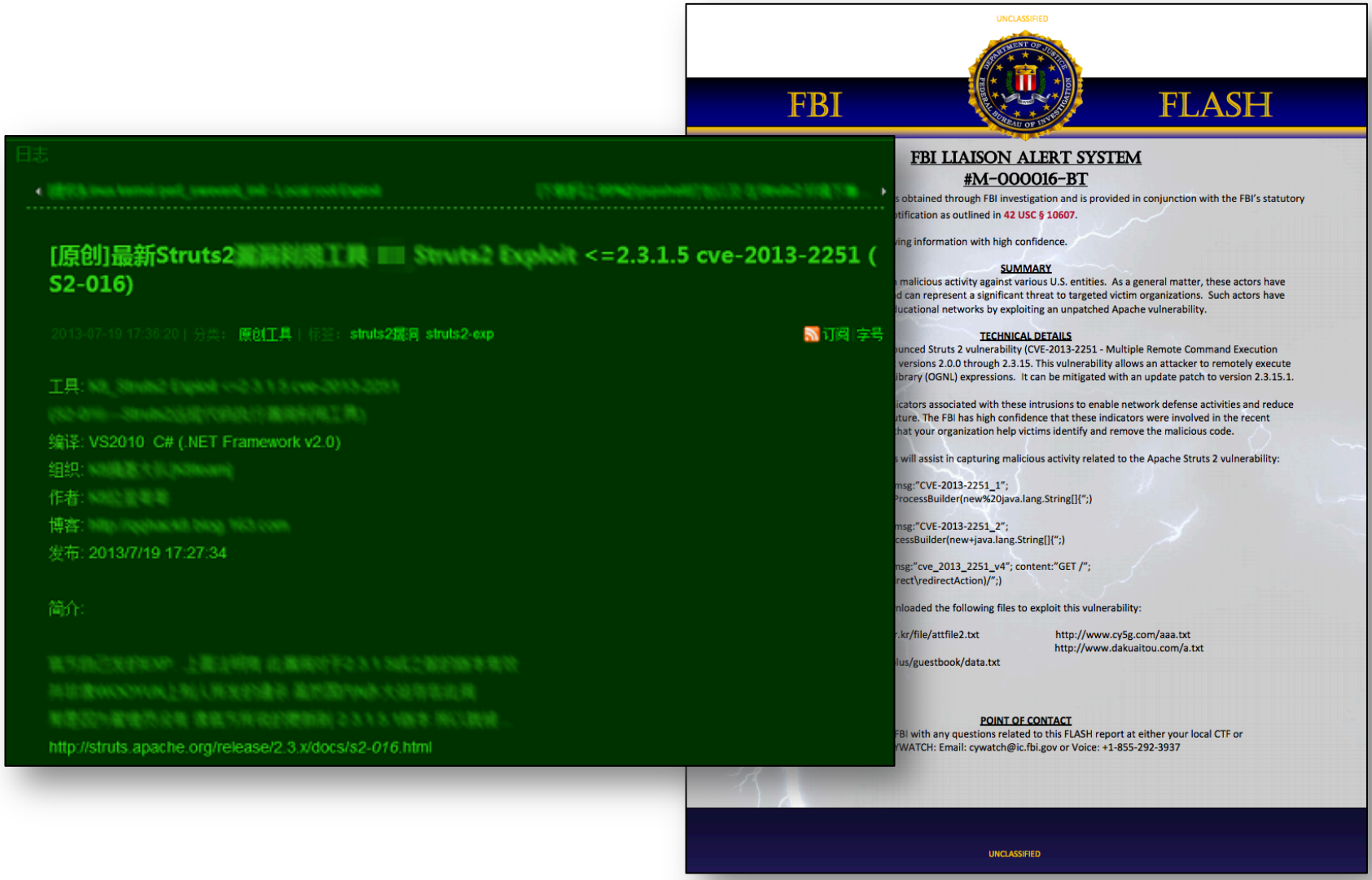
Network exploitable

Medium access complexity

No authentication required for exploit

Allows unauthorized disclosure of information; allows unauthorized modification; allows disruption of service

WIDESPREAD COMPROMISE



日志

[原创]最新Struts2 Struts2 Exploit <=2.3.1.5 cve-2013-2251 (S2-016)

2013-07-19 17:36:20 | 分类: 原创工具 | 标签: struts2漏洞 struts2-exp 订阅 | 字号

工具:

编译: VS2010 C# (.NET Framework v2.0)

组织:

作者:

博客:

发布: 2013/7/19 17:27:34

简介:

http://struts.apache.org/release/2.3.x/docs/s2-016.html

UNCLASSIFIED

FBI FLASH

FBI LIAISON ALERT SYSTEM
#M-000016-BT

s obtained through FBI investigation and is provided in conjunction with the FBI's statutory tification as outlined in 42 USC § 10607.

ing information with high confidence.

SUMMARY

malicious activity against various U.S. entities. As a general matter, these actors have d can represent a significant threat to targeted victim organizations. Such actors have ducational networks by exploiting an unpatched Apache vulnerability.

TECHNICAL DETAILS

unced Struts 2 vulnerability (CVE-2013-2251 - Multiple Remote Command Execution versions 2.0.0 through 2.3.15. This vulnerability allows an attacker to remotely execute ibrary (OGNL) expressions. It can be mitigated with an update patch to version 2.3.15.1.

icators associated with these intrusions to enable network defense activities and reduce ture. The FBI has high confidence that these indicators were involved in the recent hat your organization help victims identify and remove the malicious code.

will assist in capturing malicious activity related to the Apache Struts 2 vulnerability:

msg:"CVE-2013-2251_1";
ProcessBuilder(new%20java.lang.String[]{";)

msg:"CVE-2013-2251_2";
cessBuilder(new+java.lang.String[]{";)

sg:"cve_2013_2251_v4"; content:"GET /";
rect\redirectAction)/";)

nloaded the following files to exploit this vulnerability:

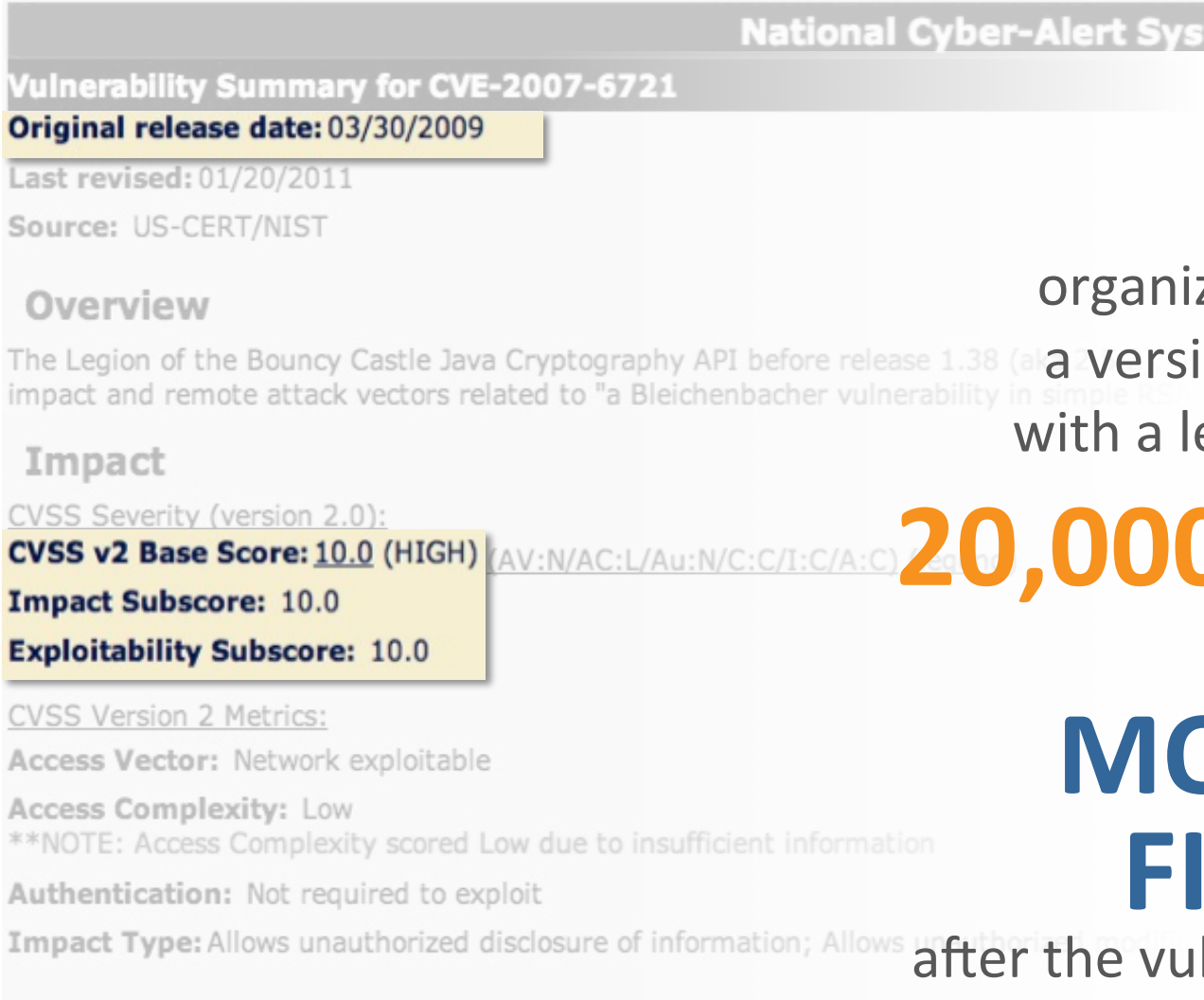
.kr/file/attfile2.txt
http://www.cy5g.com/aaa.txt
http://www.dakuaitou.com/a.txt
lus/guestbook/data.txt

POINT OF CONTACT

FBI with any questions related to this FLASH report at either your local CTF or /WATCH: Email: cywatch@ic.fbi.gov or Voice: +1-855-292-3937

UNCLASSIFIED

Sonatype

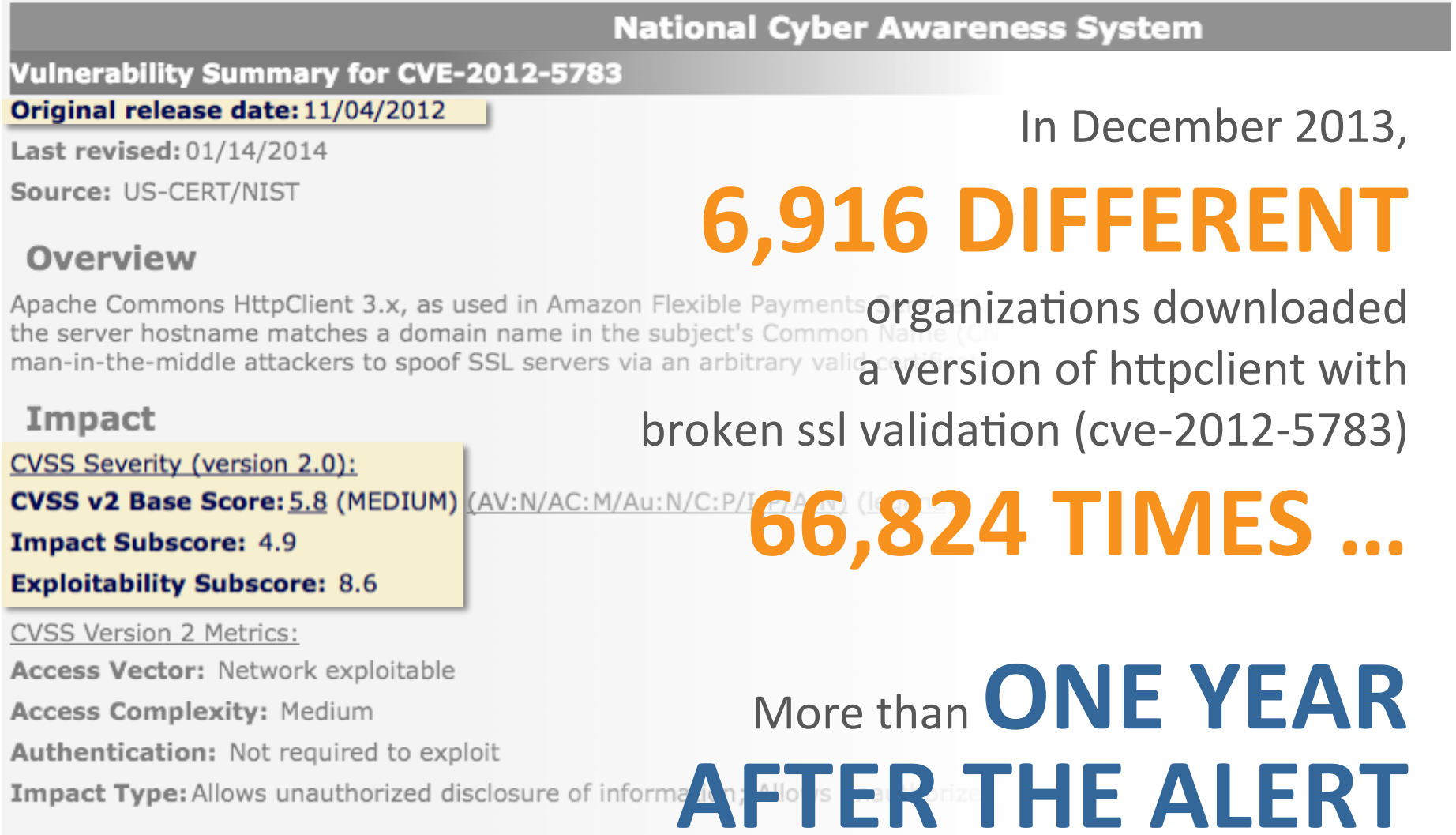


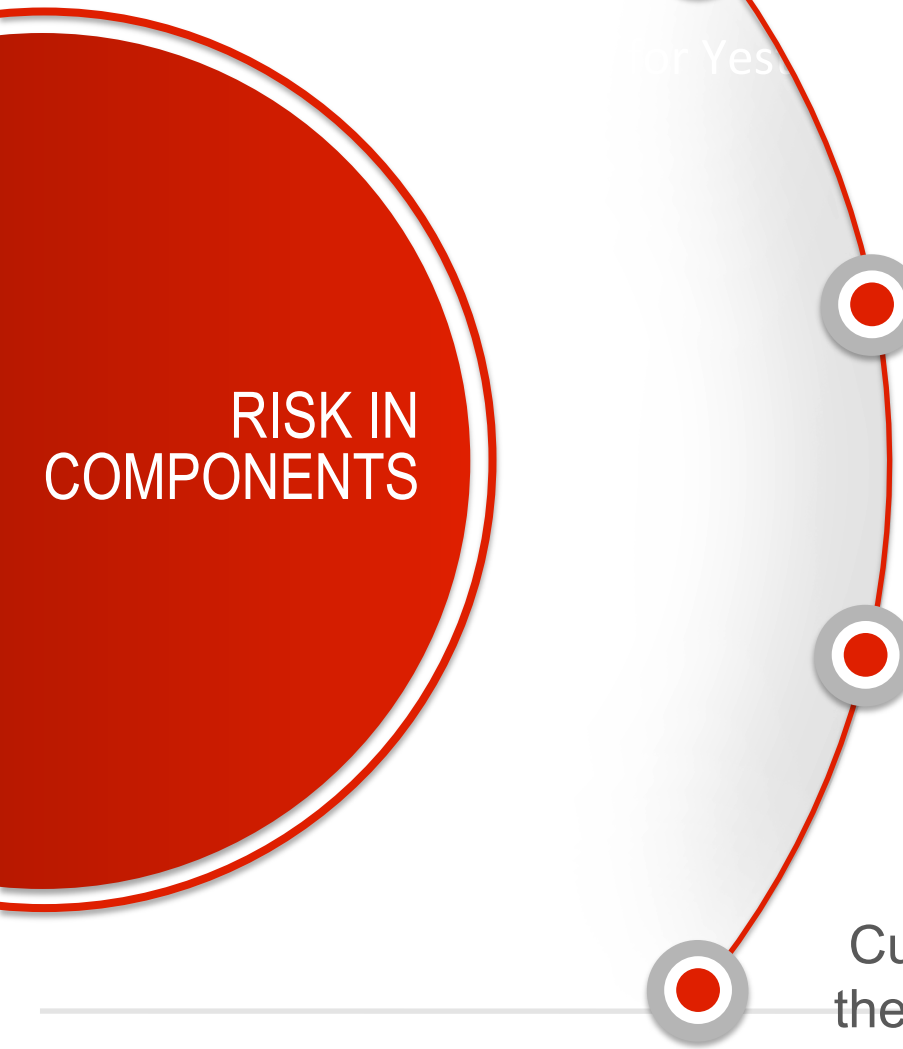
In 2013, **4,000**
organizations downloaded
a version of Bouncy Castle
with a level 10 vulnerability

20,000 TIMES …

MORE THAN FIVE YEARS

after the vulnerability was fixed


National Cyber Awareness System
Vulnerability Summary for CVE-2012-5783
Original release date: 11/04/2012
Last revised: 01/14/2014
Source: US-CERT/NIST
Overview
Apache Commons HttpClient 3.x, as used in Amazon Flexible Payments
the server hostname matches a domain name in the subject's Common
man-in-the-middle attackers to spoof SSL servers via an arbitrary
Impact
CVSS Severity (version 2.0):
CVSS v2 Base Score: 5.8 (MEDIUM)
Impact Subscore: 4.9
Exploitability Subscore: 8.6
CVSS Version 2 Metrics:
Access Vector: Network exploitable
Access Complexity: Medium
Authentication: Not required to exploit
Impact Type: Allows unauthorized disclosure of
In December 2013,
6,916 DIFFERENT
organizations downloaded
a version of httpclient with
broken ssl validation (cve-2012-5783)
66,824 TIMES ...
More than ONE YEAR
AFTER THE ALERT



Component usage has **exploded**

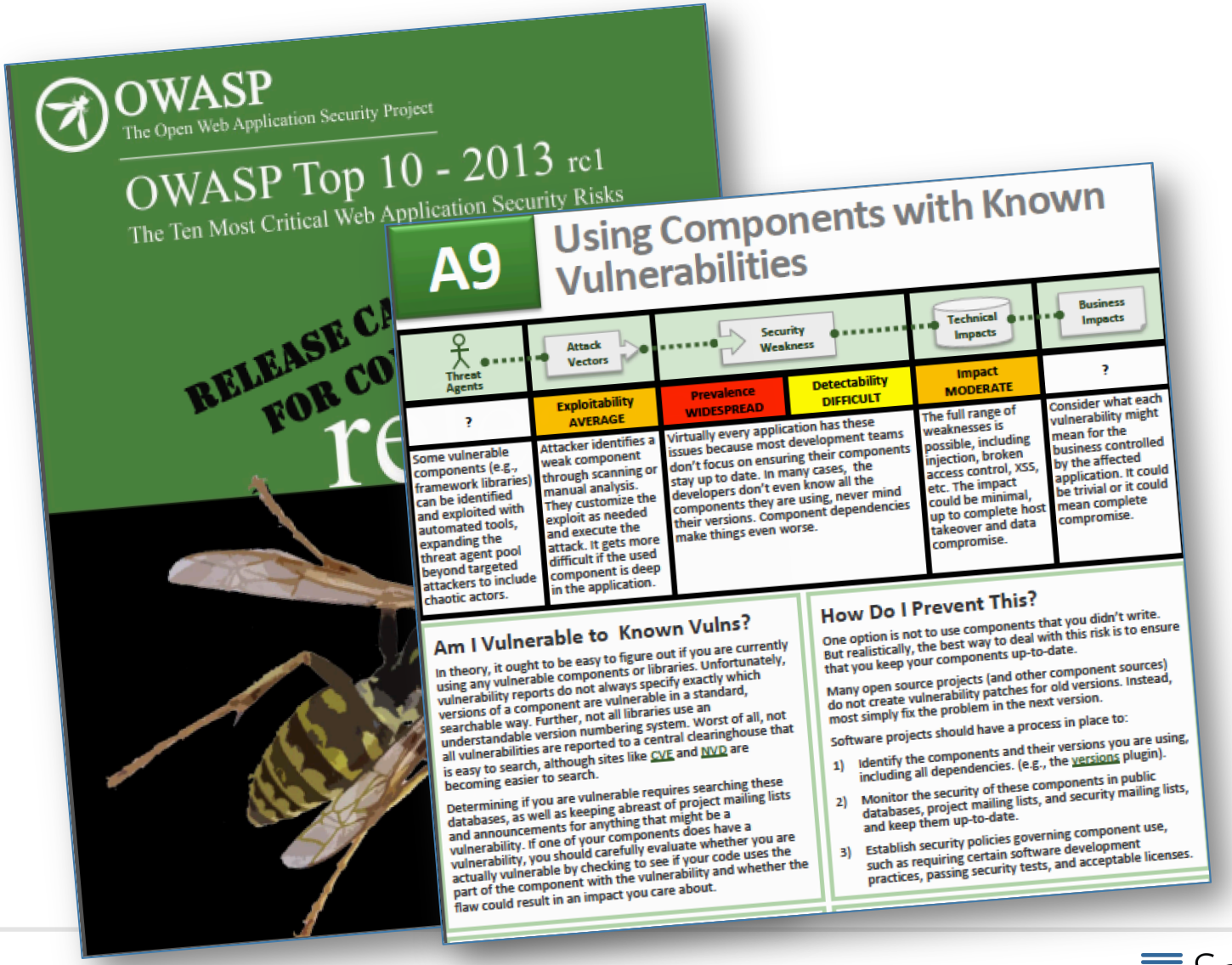
Applications are the primary vector of **attack**

There is a proliferation of **flawed** components

Current approaches **can't handle** the complexity

Sonatype

THOUGHT LEADERS ARE TAKING ACTION



Sonatype

HOW NOT TO SOLVE THIS PROBLEM

Turn off the lights!

Lock the doors!

Point fingers!

THERE IS NO PROBLEM HERE

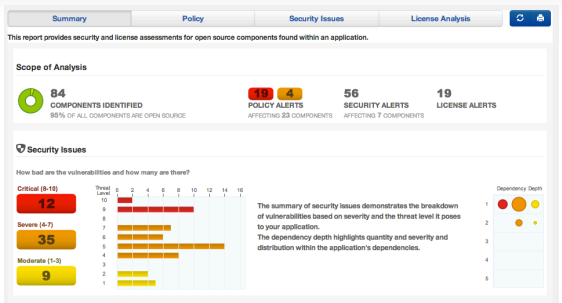
Sonatype

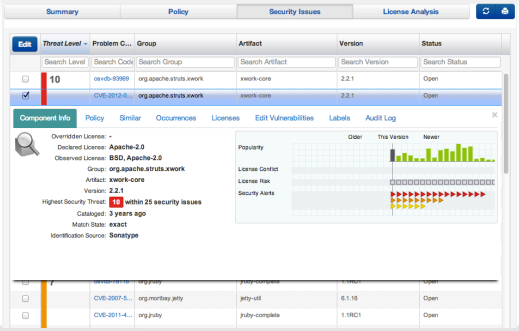
MODERN SOFTWARE PRACTICES
REQUIRE A MODERN APPROACH TO GOVERNANCE

FAST

You need to scan hundreds or thousands of applications and their transitive dependencies every day!

```
Policy(Critical Security) [
 Component(gav=commons-httpclient:commons-httpclient:3.1, hash=f0776db1593e215146d2) [
  Constraint(CVSS) [Security Vulnerability Severity >= 5 because: Found 2 Security Vulnerabilities with Severity >= 5] ],
 Component(gav=org.apache.geronimo.framework:geronimo-security:2.1, hash=848d7549ef7ec13ce546) [
  Constraint(CVSS) [Security Vulnerability Severity >= 5 because: Found 6 Security Vulnerabilities with Severity >= 5] ],
 Component(gav=org.mortbay.jetty:jetty:6.1.15, hash=494308fc2d433720c778) [
  Constraint(CVSS) [Security Vulnerability Severity >= 5 because: Found 10 Security Vulnerabilities with Severity >= 5] ],
 Component(gav=org.openid4java:openid4java:0.9.5, hash=62923bdfdfff066ea088) [
  Constraint(CVSS) [Security Vulnerability Severity >= 5 because: Found 2 Security Vulnerabilities with Severity >= 5] ],
 Component(gav=tomcat:tomcat-util:5.5.23, hash=1249e25aebb15358bedd) [
  Constraint(CVSS) [Security Vulnerability Severity >= 5 because: Found 4 Security Vulnerabilities with Severity >= 5] ]]
[DEBUG] Skipping watched dependency update for build: Sample Project #2768 due to result: FAILURE
Finished: FAIL
```





Sonatype

AUTOMATE

1. Humans define policy
2. Machines automate the implementation of policy
3. Humans manage exceptions

PRECISE

BE SPECIFIC

No Noise!

- There is a world of difference between saying "Struts is approved" and saying "Struts 2.3.15.4 is **good** and ~~Struts 2.3.15.0~~ ANY OLDER VERSION will **get your system owned**“
- Reduce the Noise Level - Provide only verified accurate information to your development teams

Scan found 50,313 “issues” ⟶

Real issue count: 204 ⟶

CONTEXTUAL

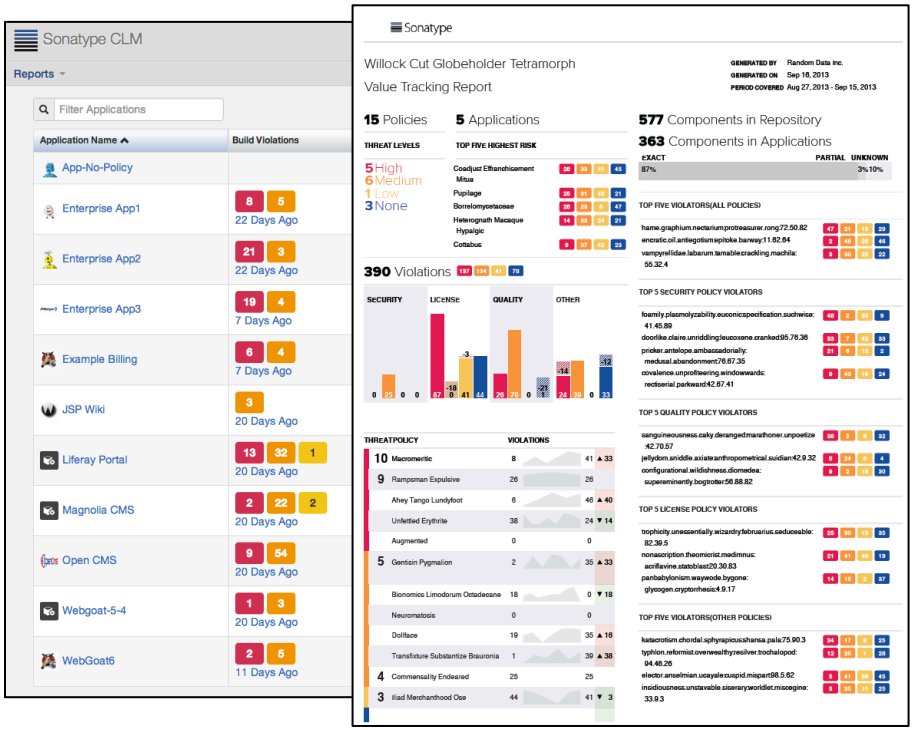
WHY CONTEXT MATTERS

- SQL Injection vulnerabilities don't affect applications without databases.
- CopyLeft may not be a problem for internal applications or services.
- I need information that applies to my application.

CONTEXTUAL

Consume information and apply policy in the context of your applications, organizations and enterprise via hierarchal policy and reporting

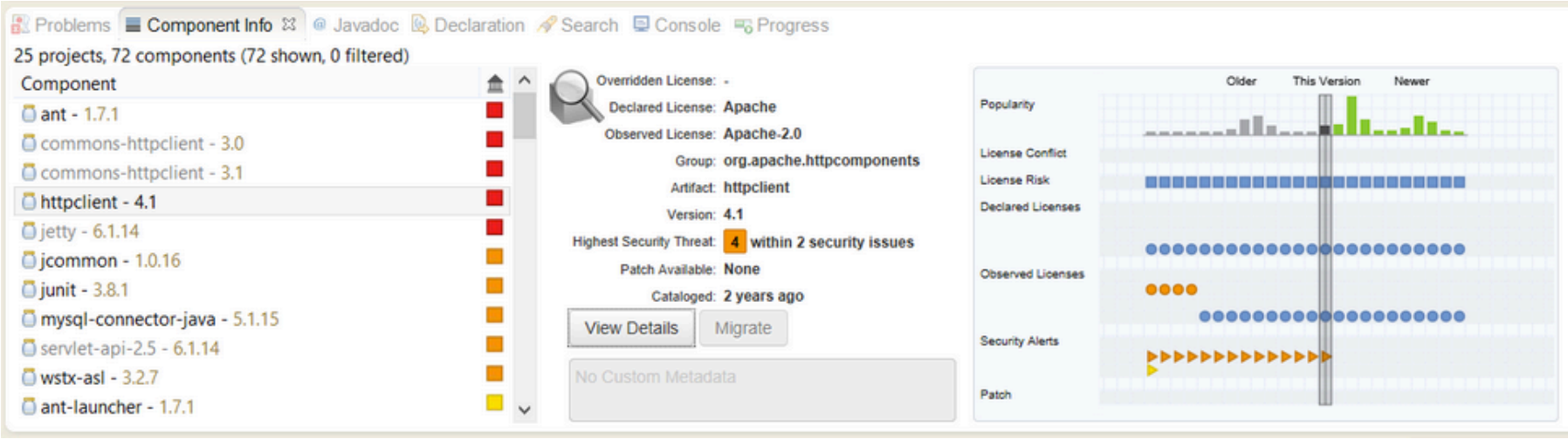
One Size does **Not** Fit All!



Sonatype

ACTIONABLE

POLICIES ENSURE DEVELOPERS START WITH RIGHT COMPONENTS



Comprehensive intelligence allows developer to start with the best component

"I can quickly pick the best component from the start, eliminating downstream rework."
Lead Developer

Sonatype

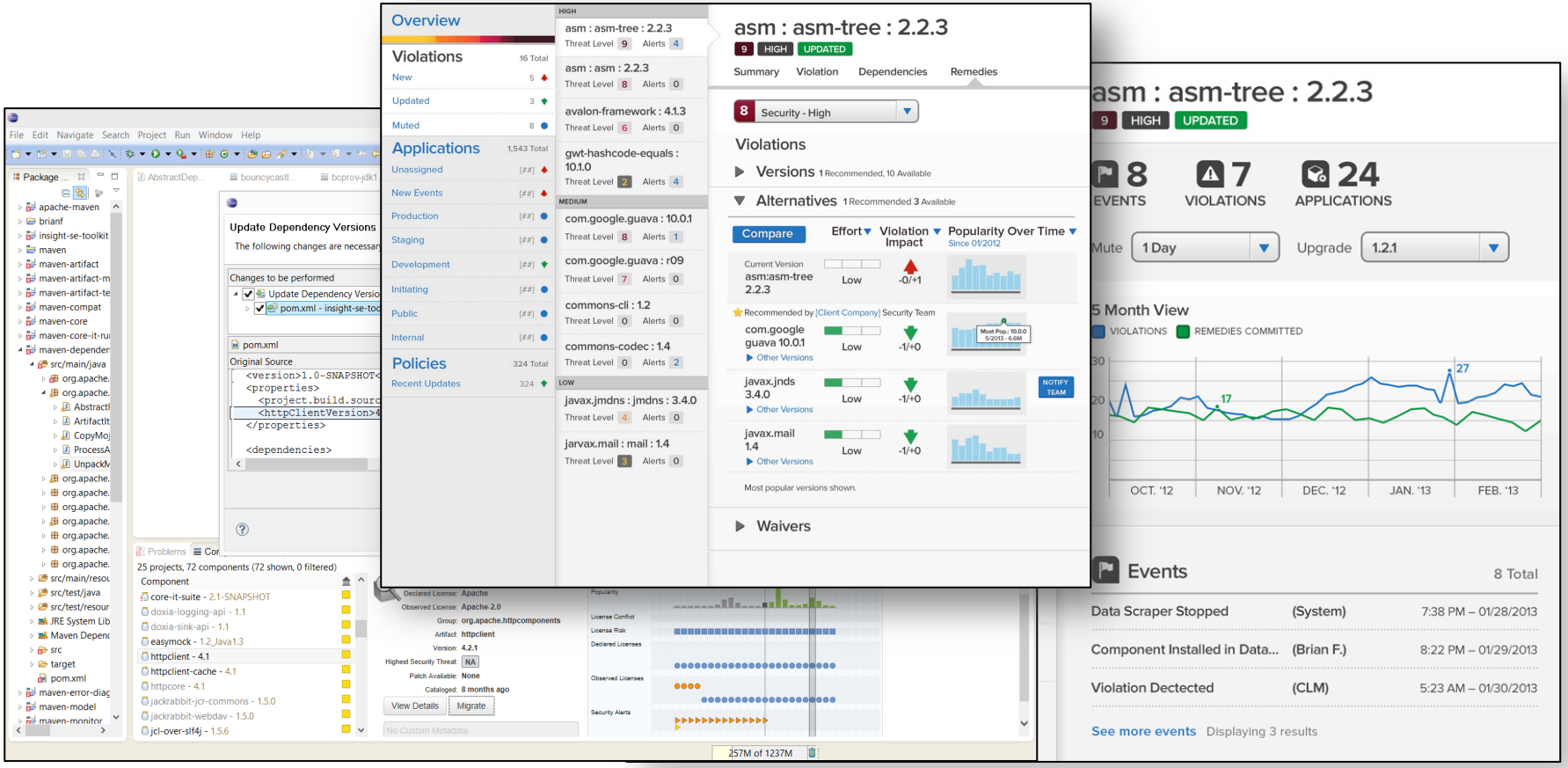
PROVIDE A SOLUTION

- Now that you've told me about a problem, tell me what I can do to fix it.
- Suggest alternatives.
- Even if I don't completely understand the risk,

  if you show me an easy fix, I will take it.

EASY TO CONSUME

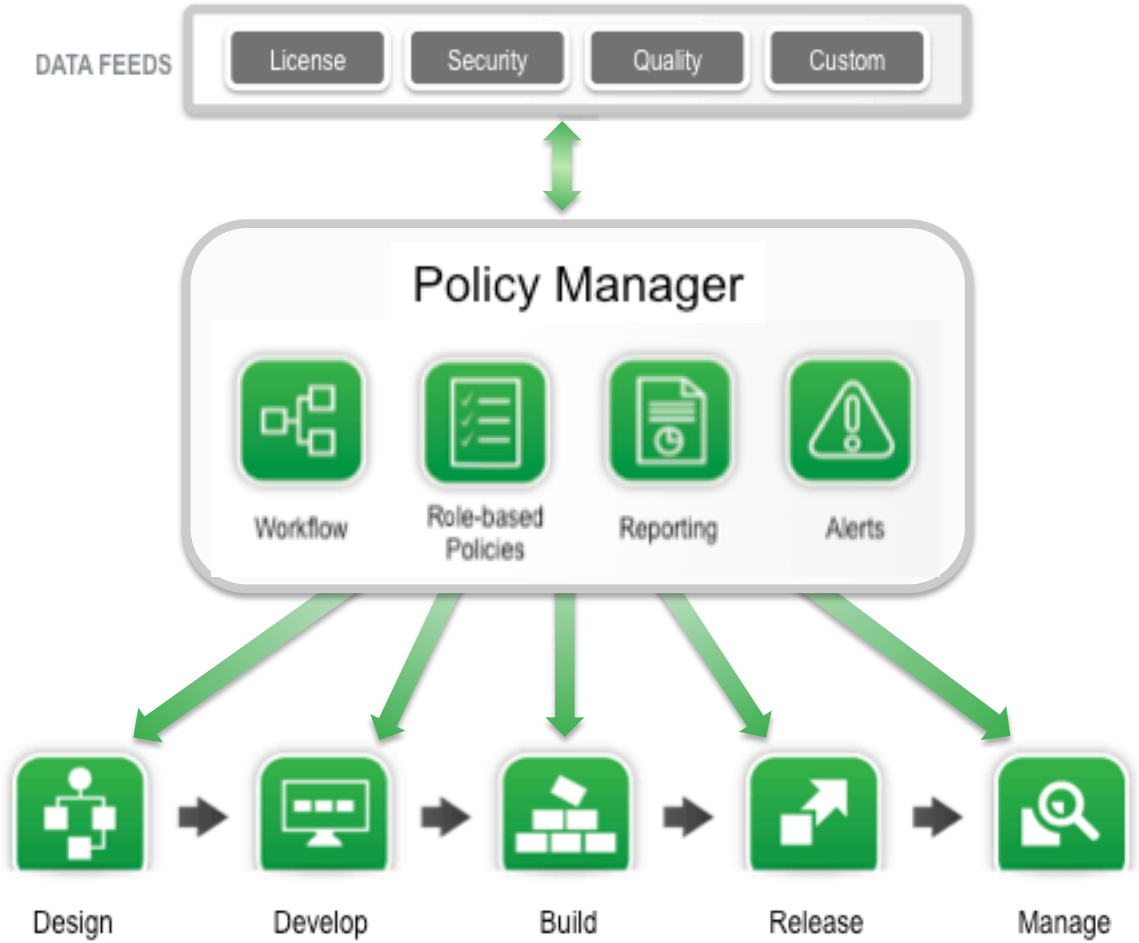
Provide stakeholders actionable, easy to consume information to remediate problems



Sonatype

CONTINUOUS

POLICIES PROVIDE FOUNDATION FOR GOVERNANCE



Centralized policy administration simplifies enterprise management

Lifecycle appropriate actions enforced automatically support a defense-in-depth strategy

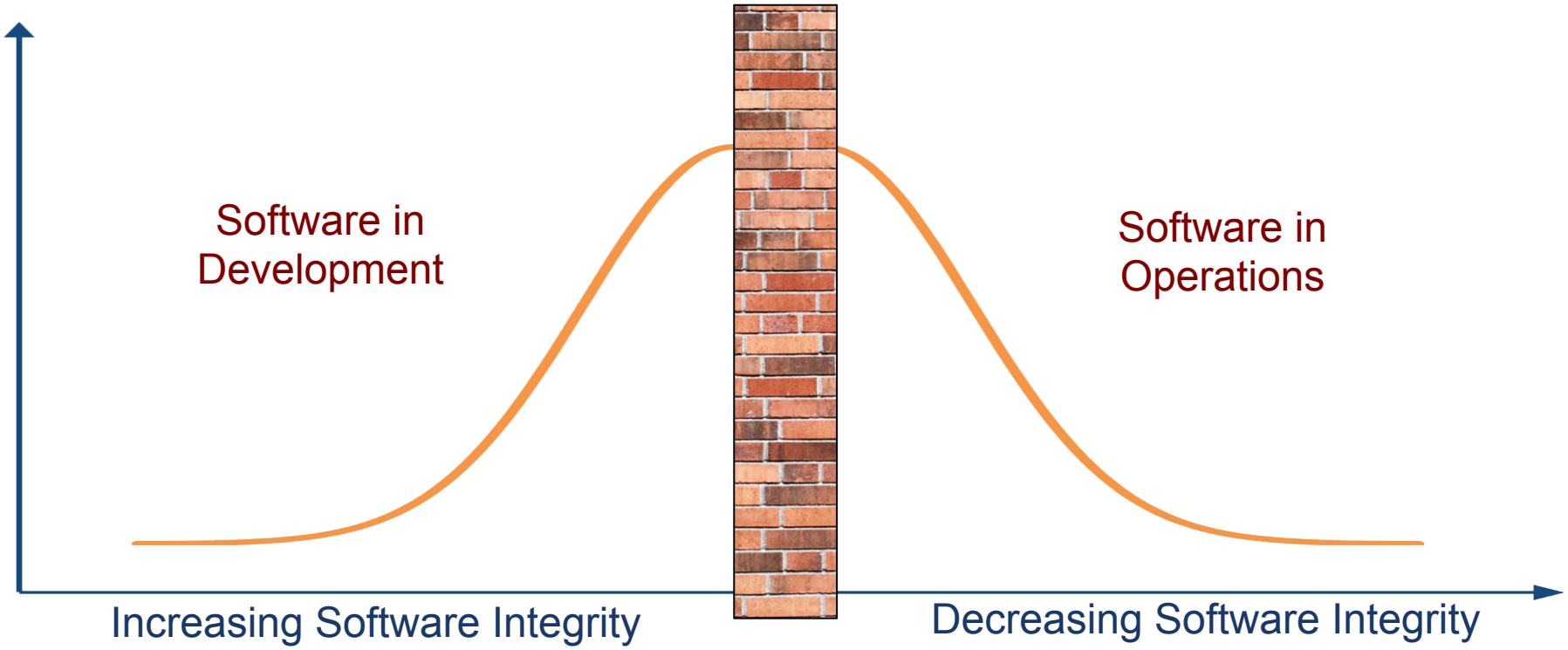
"Just by using CLM we are enforcing policy."
CISO

Sonatype

Applications don't age like wine,

THEY AGE LIKE MILK

UNMAINTAINED APPLICATIONS BECOME UNMAINTAINABLE



"It is an inconvenient reality that software integrity degrades the moment development ends."
Industry Analyst

Sonatype

SYSTEM.EXIT(0);

Q& A

Sonatype

We make it **EASY** to create

TRUSTED APPLICATIONS

and keep them that way

OVER TIME

Sonatype