



The Hidden Risk of OSS

The Dawn of Software Assembly





The Language of Security is Risk





What is Risk



**“...WE OWE A DUTY OF
REASONABLE CARE TO
OUR NEIGHBOR”**

Lord Atkin: *Donoghue v. Stevenson* (1932)

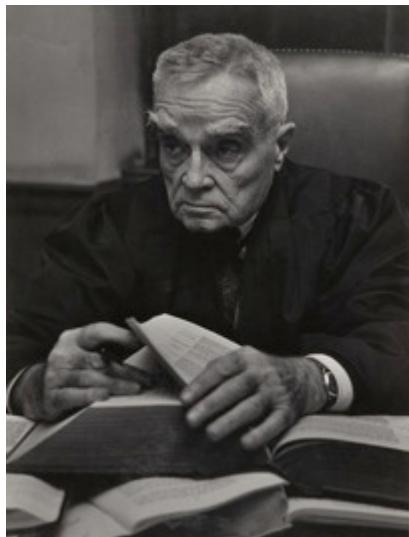
“...a manufacturer of products, which he sells in such a form as to show that he intends them to reach the ultimate consumer in the form in which they left him with no reasonable possibility of intermediate examination, and with knowledge that the absence of reasonable care in the preparation or putting up of products will result in an injury to the consumer's life or property, owes a duty to the consumer to take that reasonable care.”



“IT (BUICK) WAS NOT AT LIBERTY TO PUT THE FINISHED PRODUCT ON THE MARKET WITHOUT SUBJECTING THE COMPONENT PARTS TO ORDINARY AND SIMPLE TESTS....THE OBLIGATION TO INSPECT MUST VARY WITH THE NATURE OF THE THING TO BE INSPECTED. THE MORE PROBABLE THE DANGER, THE GREATER THE NEED OF CAUTION.”

MacPherson v. Buick Motor Company,
217 N.Y. 382, 111 N.E. 1050 (1916)
Justice Benjamin N. Cardozo

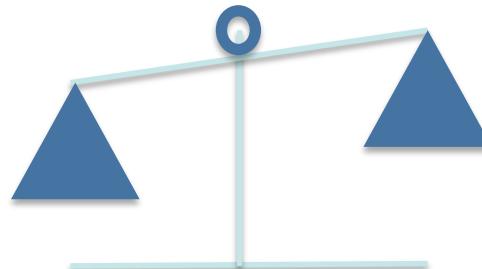
“...IF THE PROBABILITY BE CALLED P; THE INJURY, L; AND THE BURDEN, B; LIABILITY DEPENDS UPON WHETHER B IS LESS THAN L MULTIPLIED BY P: I.E., WHETHER $B < PL$ ”.



United States v. Carroll Towing Co.
159 F.2d 169 (2d. Cir. 1947)

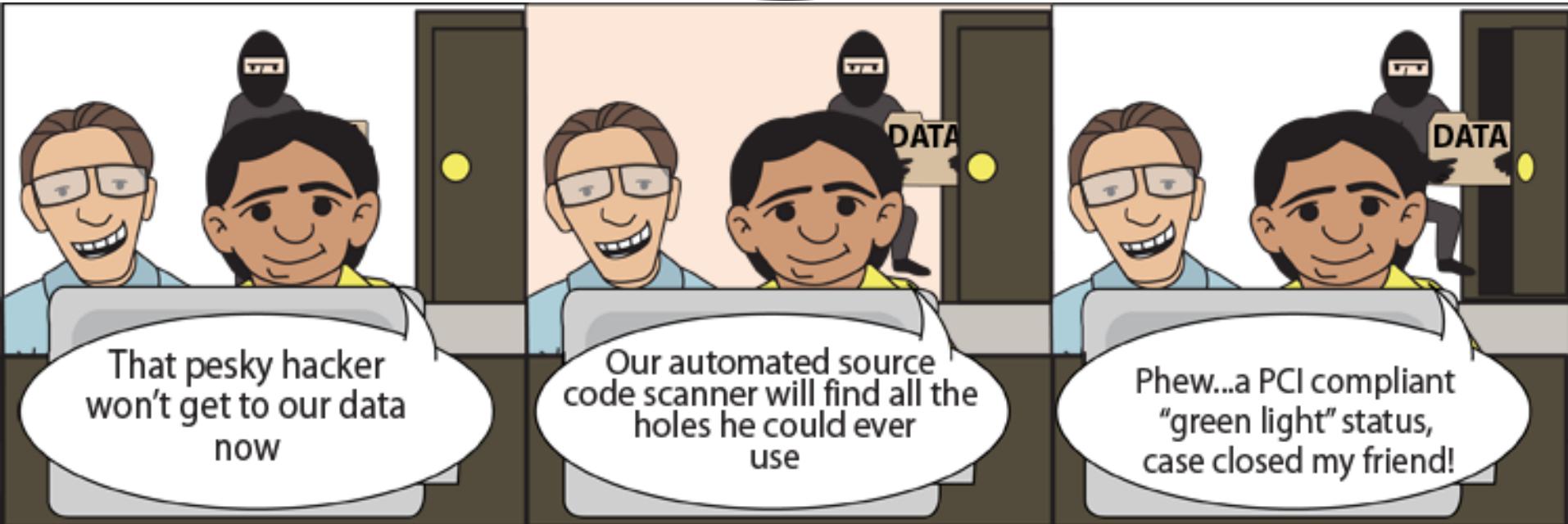
Translation: If the Cost of Protecting Against Harm is less than the Cost of the Damage Multiplied by the Likelihood of the Damage, then there is **negligence**.

Risk = probability x impact



Security concerns are across the Enterprise

Development	Operations	Security
Features	Performance	Security
Usability	Reliability/Scalability	Compliance
Performance	Compliance	Everything Else
Reliability/Scalability	Security	
Maintainability	Maintainability	
Security	Features/Usability	
Compliance		



Prevention	Detection	Monitoring
Firewall	IDS	SIEM
Encryption	SAST	DAM
IPS	DAST	RAST
WebApp Firewall (WAF)		

Evolution of Spend

Figure 1. Magic Quadrant for Dynamic Application Security Testing



Source: Gartner (December 2011)

DAST is a very mature market, but is focused primarily late in the development cycle and not integrated into development.

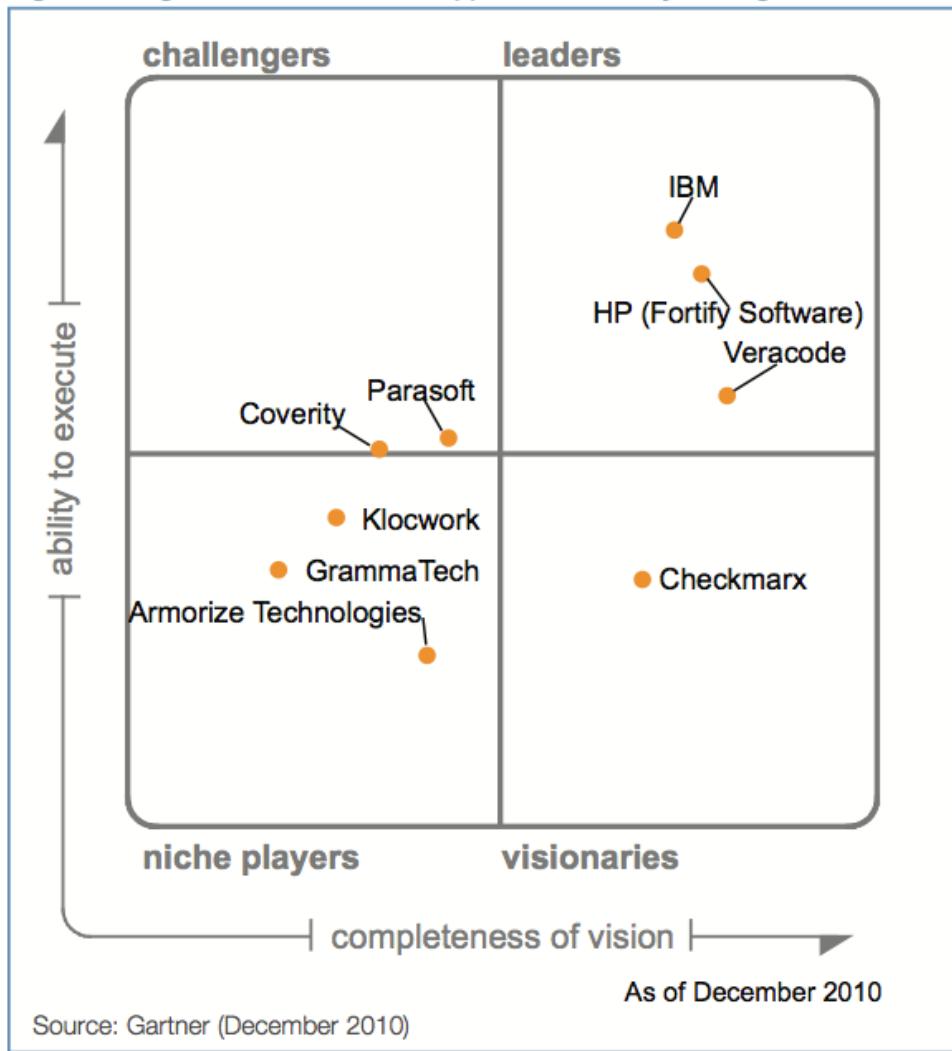
Pros

- Finds exploitable issues
- Mostly language agnostic
- Finds some infrastructure issues

Cons

- Often requires complex configuration
- Accuracy drops for non-reflected issues
- Used late in SDLC

Figure 1. Magic Quadrant for Static Application Security Testing



SAST is a mature market, but is under represented outside of financial, health/insurance and retail markets.

Pros

- Can be leveraged early in the development lifecycle
- Can find issues not found using any DAST

Cons

- False Positives
- Requires security training to use effectively.
- Scanning varies from hours to days for large applications.

Over the past decade there have been two predominant security technologies focused at application security.

- DAST – Dynamic Application Security Testing (Blackbox)
- SAST – Static Application Security Testing (Whitebox)

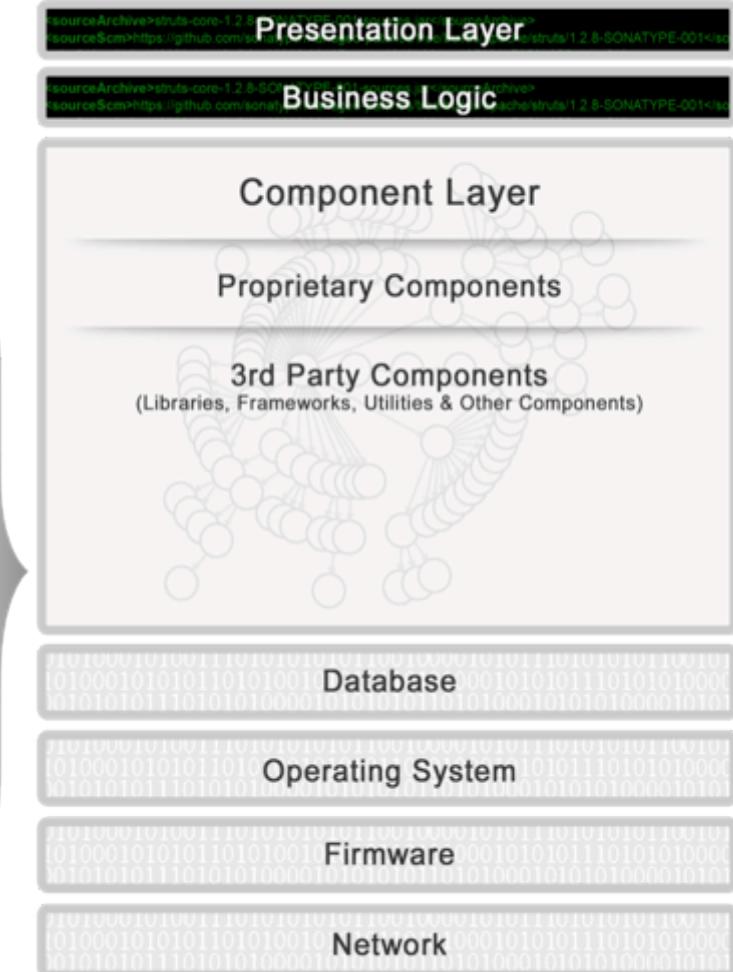
Over the last couple of years a third has emerged but has not gained significant adoption

- RAST – Runtime Application Security Testing (Glassbox)

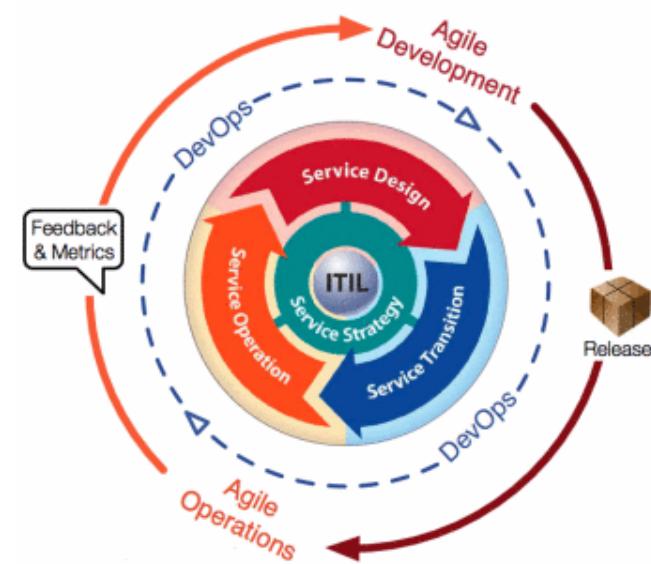
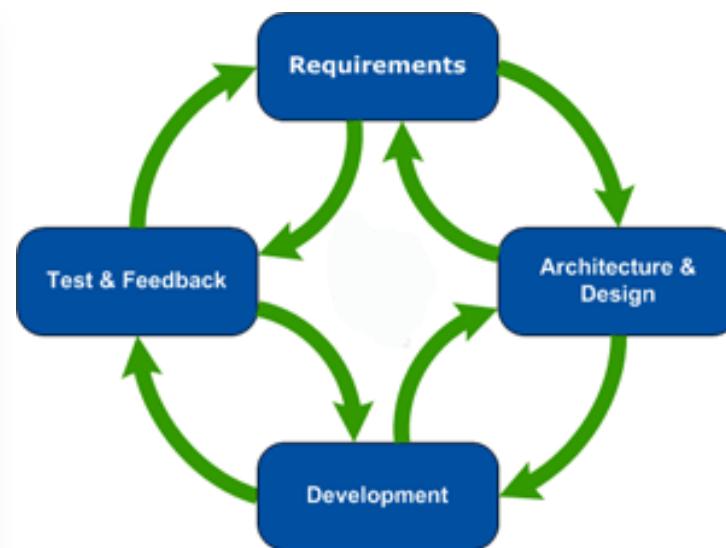


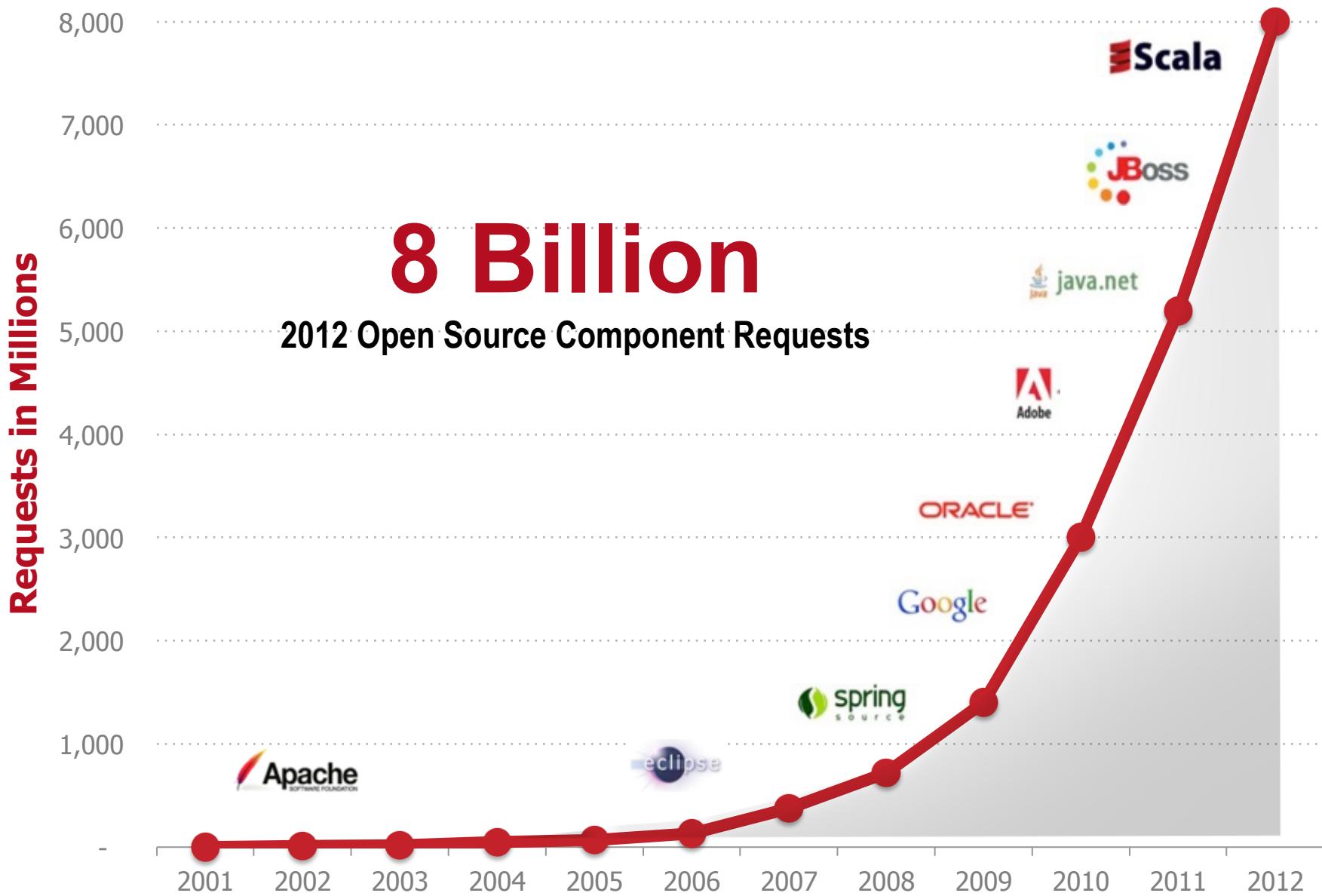
A Sea Change in Application Development

Assembled 90%

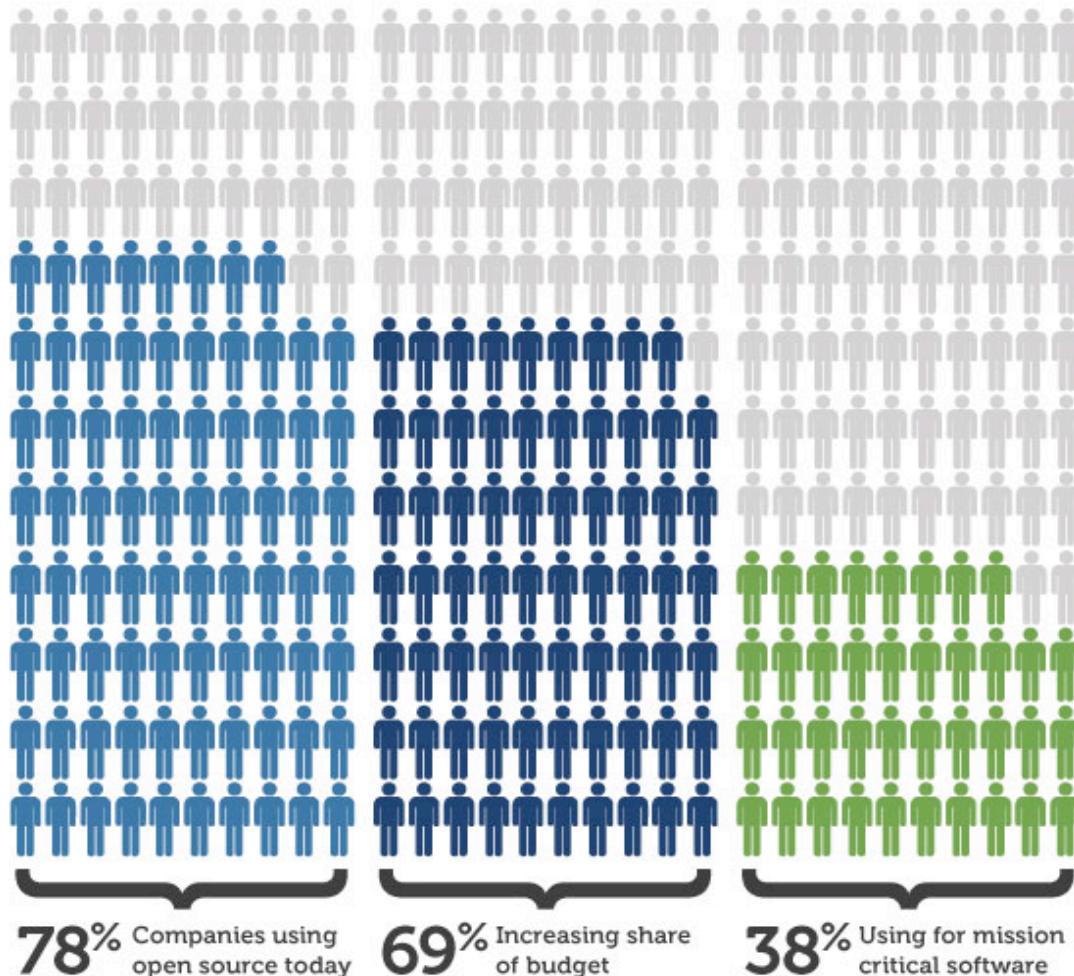


Development must change

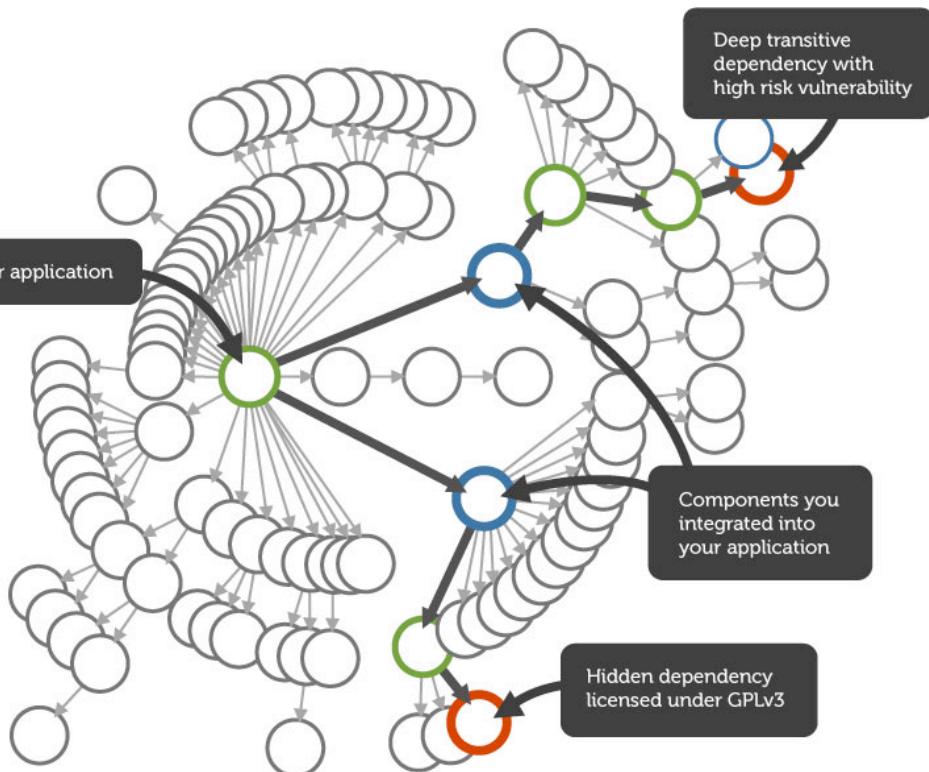




Usage of OSS in large enterprises



It's no longer a question of whether you use OSS, it's how many components are being used & where



- Discovering a security issue is half the battle
- Transitive and hidden dependencies make it extremely difficult to assign responsibility to propagate fixes throughout the component chain



Complexity

One component may
rely on 00s
of others



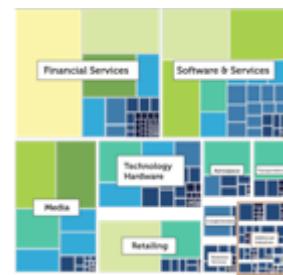
Diversity

40,000 Projects
200MM Classes
400K Components



Volume

Typical Enterprise
Consumes
000s of
Components Monthly



Change

Typical Component
is Updated 4X
per Year

Component ID	Timestamp
Comp111	01 April 2012
Comp112	20 January 2012
Comp113	20 December 2011
Comp114	01 January 2012
Comp115	01 July 2012
Comp116	01 October 2012
Comp117	01 November 2012
Comp118	01 December 2012
Comp119	01 January 2013
Comp120	01 August 2012
Comp121	01 November 2012
Comp122	01 December 2012
Comp123	01 January 2013
Comp124	01 February 2013
Comp125	01 March 2013
Comp126	01 April 2013
Comp127	01 May 2013
Comp128	01 June 2013
Comp129	01 July 2013
Comp130	01 August 2013
Comp131	01 September 2013
Comp132	01 October 2013
Comp133	01 November 2013
Comp134	01 December 2013
Comp135	01 January 2014
Comp136	01 February 2014
Comp137	01 March 2014
Comp138	01 April 2014
Comp139	01 May 2014
Comp140	01 June 2014
Comp141	01 July 2014
Comp142	01 August 2014
Comp143	01 September 2014
Comp144	01 October 2014
Comp145	01 November 2014
Comp146	01 December 2014
Comp147	01 January 2015
Comp148	01 February 2015
Comp149	01 March 2015
Comp150	01 April 2015
Comp151	01 May 2015
Comp152	01 June 2015
Comp153	01 July 2015
Comp154	01 August 2015
Comp155	01 September 2015
Comp156	01 October 2015
Comp157	01 November 2015
Comp158	01 December 2015
Comp159	01 January 2016
Comp160	01 February 2016
Comp161	01 March 2016
Comp162	01 April 2016
Comp163	01 May 2016
Comp164	01 June 2016
Comp165	01 July 2016
Comp166	01 August 2016
Comp167	01 September 2016
Comp168	01 October 2016
Comp169	01 November 2016
Comp170	01 December 2016
Comp171	01 January 2017
Comp172	01 February 2017
Comp173	01 March 2017
Comp174	01 April 2017
Comp175	01 May 2017
Comp176	01 June 2017
Comp177	01 July 2017
Comp178	01 August 2017
Comp179	01 September 2017
Comp180	01 October 2017
Comp181	01 November 2017
Comp182	01 December 2017
Comp183	01 January 2018
Comp184	01 February 2018
Comp185	01 March 2018
Comp186	01 April 2018
Comp187	01 May 2018
Comp188	01 June 2018
Comp189	01 July 2018
Comp190	01 August 2018
Comp191	01 September 2018
Comp192	01 October 2018
Comp193	01 November 2018
Comp194	01 December 2018
Comp195	01 January 2019
Comp196	01 February 2019
Comp197	01 March 2019
Comp198	01 April 2019
Comp199	01 May 2019
Comp200	01 June 2019
Comp201	01 July 2019
Comp202	01 August 2019
Comp203	01 September 2019
Comp204	01 October 2019
Comp205	01 November 2019
Comp206	01 December 2019
Comp207	01 January 2020
Comp208	01 February 2020
Comp209	01 March 2020
Comp210	01 April 2020
Comp211	01 May 2020
Comp212	01 June 2020
Comp213	01 July 2020
Comp214	01 August 2020
Comp215	01 September 2020
Comp216	01 October 2020
Comp217	01 November 2020
Comp218	01 December 2020
Comp219	01 January 2021
Comp220	01 February 2021
Comp221	01 March 2021
Comp222	01 April 2021
Comp223	01 May 2021
Comp224	01 June 2021
Comp225	01 July 2021
Comp226	01 August 2021
Comp227	01 September 2021
Comp228	01 October 2021
Comp229	01 November 2021
Comp230	01 December 2021
Comp231	01 January 2022
Comp232	01 February 2022
Comp233	01 March 2022
Comp234	01 April 2022
Comp235	01 May 2022
Comp236	01 June 2022
Comp237	01 July 2022
Comp238	01 August 2022
Comp239	01 September 2022
Comp240	01 October 2022
Comp241	01 November 2022
Comp242	01 December 2022
Comp243	01 January 2023
Comp244	01 February 2023
Comp245	01 March 2023
Comp246	01 April 2023
Comp247	01 May 2023
Comp248	01 June 2023
Comp249	01 July 2023
Comp250	01 August 2023
Comp251	01 September 2023
Comp252	01 October 2023
Comp253	01 November 2023
Comp254	01 December 2023
Comp255	01 January 2024
Comp256	01 February 2024
Comp257	01 March 2024
Comp258	01 April 2024
Comp259	01 May 2024
Comp260	01 June 2024
Comp261	01 July 2024
Comp262	01 August 2024
Comp263	01 September 2024
Comp264	01 October 2024
Comp265	01 November 2024
Comp266	01 December 2024
Comp267	01 January 2025
Comp268	01 February 2025
Comp269	01 March 2025
Comp270	01 April 2025
Comp271	01 May 2025
Comp272	01 June 2025
Comp273	01 July 2025
Comp274	01 August 2025
Comp275	01 September 2025
Comp276	01 October 2025
Comp277	01 November 2025
Comp278	01 December 2025
Comp279	01 January 2026
Comp280	01 February 2026
Comp281	01 March 2026
Comp282	01 April 2026
Comp283	01 May 2026
Comp284	01 June 2026
Comp285	01 July 2026
Comp286	01 August 2026
Comp287	01 September 2026
Comp288	01 October 2026
Comp289	01 November 2026
Comp290	01 December 2026
Comp291	01 January 2027
Comp292	01 February 2027
Comp293	01 March 2027
Comp294	01 April 2027
Comp295	01 May 2027
Comp296	01 June 2027
Comp297	01 July 2027
Comp298	01 August 2027
Comp299	01 September 2027
Comp300	01 October 2027
Comp301	01 November 2027
Comp302	01 December 2027
Comp303	01 January 2028
Comp304	01 February 2028
Comp305	01 March 2028
Comp306	01 April 2028
Comp307	01 May 2028
Comp308	01 June 2028
Comp309	01 July 2028
Comp310	01 August 2028
Comp311	01 September 2028
Comp312	01 October 2028
Comp313	01 November 2028
Comp314	01 December 2028
Comp315	01 January 2029
Comp316	01 February 2029
Comp317	01 March 2029
Comp318	01 April 2029
Comp319	01 May 2029
Comp320	01 June 2029
Comp321	01 July 2029
Comp322	01 August 2029
Comp323	01 September 2029
Comp324	01 October 2029
Comp325	01 November 2029
Comp326	01 December 2029
Comp327	01 January 2030
Comp328	01 February 2030
Comp329	01 March 2030
Comp330	01 April 2030
Comp331	01 May 2030
Comp332	01 June 2030
Comp333	01 July 2030
Comp334	01 August 2030
Comp335	01 September 2030
Comp336	01 October 2030
Comp337	01 November 2030
Comp338	01 December 2030
Comp339	01 January 2031
Comp340	01 February 2031
Comp341	01 March 2031
Comp342	01 April 2031
Comp343	01 May 2031
Comp344	01 June 2031
Comp345	01 July 2031
Comp346	01 August 2031
Comp347	01 September 2031
Comp348	01 October 2031
Comp349	01 November 2031
Comp350	01 December 2031
Comp351	01 January 2032
Comp352	01 February 2032
Comp353	01 March 2032
Comp354	01 April 2032
Comp355	01 May 2032
Comp356	01 June 2032
Comp357	01 July 2032
Comp358	01 August 2032
Comp359	01 September 2032
Comp360	01 October 2032
Comp361	01 November 2032
Comp362	01 December 2032
Comp363	01 January 2033
Comp364	01 February 2033
Comp365	01 March 2033
Comp366	01 April 2033
Comp367	01 May 2033
Comp368	01 June 2033
Comp369	01 July 2033
Comp370	01 August 2033
Comp371	01 September 2033
Comp372	01 October 2033
Comp373	01 November 2033
Comp374	01 December 2033
Comp375	01 January 2034
Comp376	01 February 2034
Comp377	01 March 2034
Comp378	01 April 2034
Comp379	01 May 2034
Comp380	01 June 2034
Comp381	01 July 2034
Comp382	01 August 2034
Comp383	01 September 2034
Comp384	01 October 2034
Comp385	01 November 2034
Comp386	01 December 2034
Comp387	01 January 2035
Comp388	01 February 2035
Comp389	01 March 2035
Comp390	01 April 2035
Comp391	01 May 2035
Comp392	01 June 2035
Comp393	01 July 2035
Comp394	01 August 2035
Comp395	01 September 2035
Comp396	01 October 2035
Comp397	01 November 2035
Comp398	01 December 2035
Comp399	01 January 2036
Comp400	01 February 2036
Comp401	01 March 2036
Comp402	01 April 2036
Comp403	01 May 2036
Comp404	01 June 2036
Comp405	01 July 2036
Comp406	01 August 2036
Comp407	01 September 2036
Comp408	01 October 2036
Comp409	01 November 2036
Comp410	01 December 2036
Comp411	01 January 2037
Comp412	01 February 2037
Comp413	01 March 2037
Comp414	01 April 2037
Comp415	01 May 2037
Comp416	01 June 2037
Comp417	01 July 2037
Comp418	01 August 2037
Comp419	01 September 2037
Comp420	01 October 2037
Comp421	01 November 2037
Comp422	01 December 2037
Comp423	01 January 2038
Comp424	01 February 2038
Comp425	01 March 2038
Comp426	01 April 2038
Comp427	01 May 2038
Comp428	01 June 2038
Comp429	01 July 2038
Comp430	01 August 2038
Comp431	01 September 2038
Comp432	01 October 2038
Comp433	01 November 2038
Comp434	01 December 2038
Comp435	01 January 2039
Comp436	01 February 2039
Comp437	01 March 2039
Comp438	01 April 2039
Comp439	01 May 2039
Comp440	01 June 2039
Comp441	01 July 2039
Comp442	01 August 2039
Comp443	01 September 2039
Comp444	01 October 2039
Comp445	01 November 2039
Comp446	01 December 2039
Comp447	01 January 2040
Comp448	01 February 2040
Comp449	01 March 2040
Comp450	01 April 2040
Comp451	01 May 2040
Comp452	01 June 2040
Comp453	01 July 2040
Comp454	01 August 2040
Comp455	01 September 2040
Comp456	01 October 2040
Comp457	01 November 2040
Comp458	01 December 2040
Comp459	01 January 2041
Comp460	01 February 2041
Comp461	01 March 2041
Comp462	01 April 2041
Comp463	01 May 2041
Comp464	01 June 2041
Comp465	01 July 2041
Comp466	01 August 2041
Comp467	01 September 2041
Comp468	01 October 2041
Comp469	01 November 2041
Comp470	01 December 2041
Comp471	01 January 2042
Comp472	01 February 2042
Comp473	01 March 2042
Comp474	01 April 2042
Comp475	01 May 2042
Comp476	01 June 2042
Comp477	01 July 2042
Comp478	01 August 2042
Comp479	01 September 2042
Comp480	01 October 2042
Comp481	01 November 2042
Comp482	01 December 2042
Comp483	01 January 2043
Comp484	01 February 2043
Comp485	01 March 2043
Comp486	01 April 2043
Comp487	01 May 2043
Comp488	01 June 2043
Comp489	01 July 2043
Comp490	01 August 2043
Comp491	01 September 2043
Comp492	01 October 2043
Comp493	01 November 2043
Comp494	01 December 2043
Comp495	01 January 2044
Comp496	01 February 2044
Comp497	01 March 2044
Comp498	01 April 2044
Comp499	01 May 2044
Comp500	01 June 2044



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.



**46
Million**

Insecure downloads in 2012

**18
Thousand**

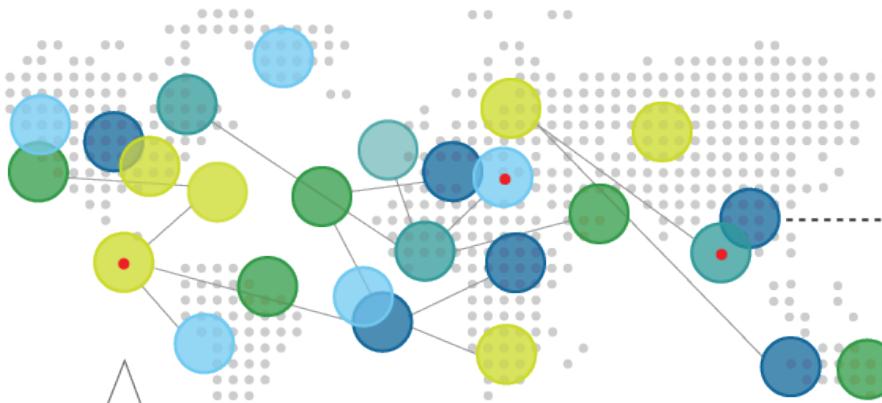
organizations downloaded Struts framework with "severe" security flaw

**4
Thousand**

organizations downloaded Struts 1.x with known security flaws



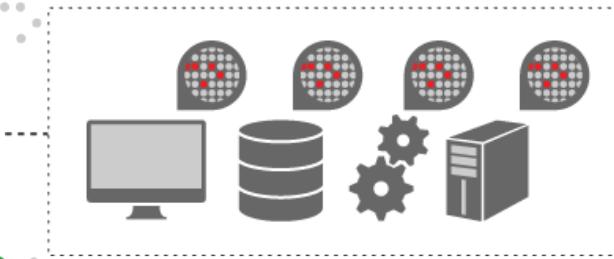
Extended Software Supply Chain



46 million

insecure component
downloads in 2012

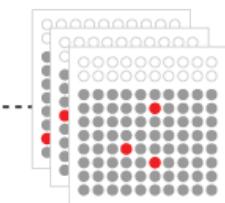
Enterprise Software Factory



90 %

of repositories contain at least
one **Critical** vulnerability
in their direct dependencies

Production Apps



71 %

of applications
contain **Critical**
or **Severe**
security flaws



Success Requires Discipline





The Problem is Not Problem Discovery



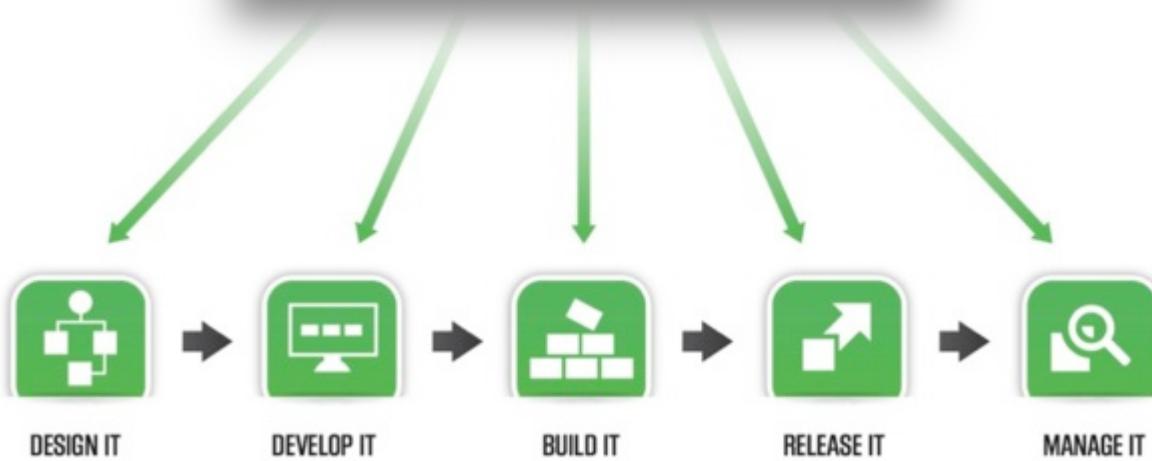
- When our software development ecosystem looks like this it is easy to find problems
- The real challenge is to develop at scale and deliver continuous value continuously when everything else is a mess



Go Fast, Be Secure



“Haven’t I heard this story before?”





Component Lifecycle Management

1

Secure Consumption
with the use of certified components & integrity checking throughout the lifecycle

2

Govern Development
to ensure policy compliance without disrupting developer productivity

3

Profile Exposures
to proactively identify and prioritize action

4

Remediate Risk
by preventing & quickly fixing security & IP vulnerabilities

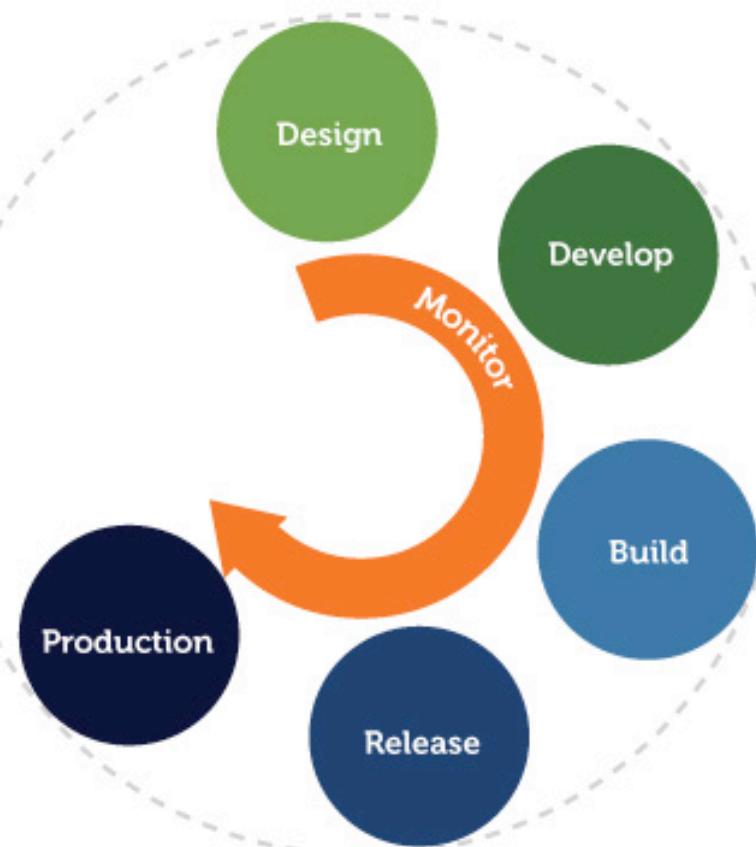
5

Monitor Threats
in production applications to ensure continuous trust in critical operations

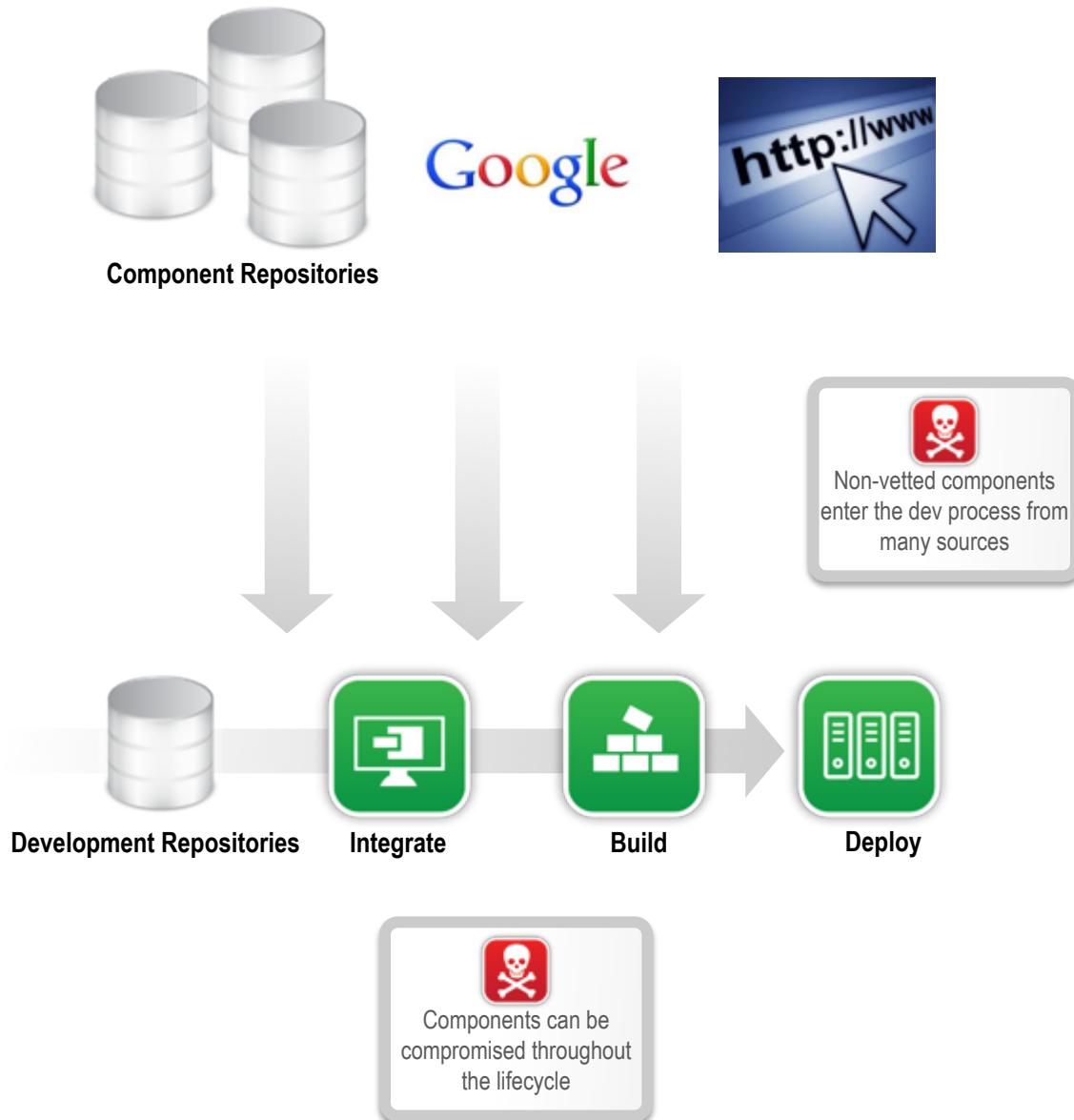




You Have to Ask the Right Questions

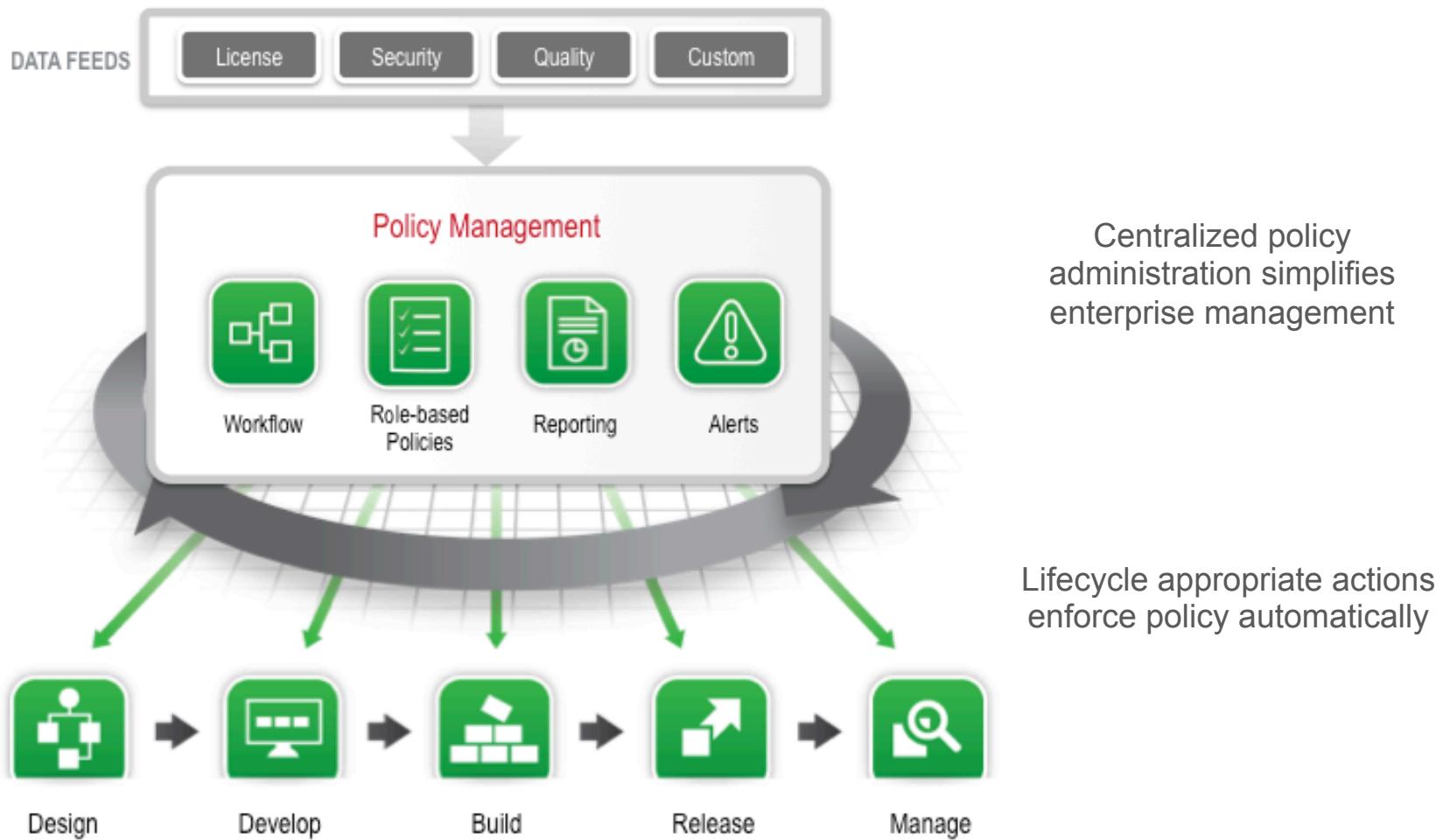


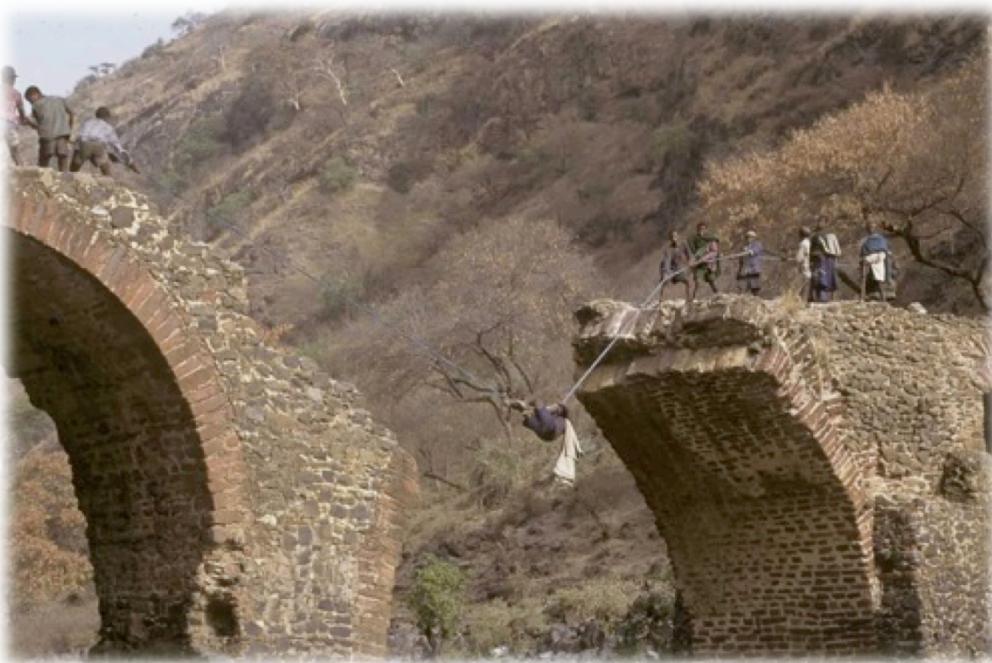
- Q** How do you choose components to include in your application?
A Thoughtfully select and identify components using quality, security, and licensing information.
- Q** How do your developers know what components to use, and when they should upgrade?
A Provide your team with real-time information and updates directly within the tools they use every day.
- Q** Do you monitor and control what makes it into a build?
A Enforce policy through your build and continuous integration infrastructure.
- Q** Do you know your full bill of materials?
A Develop and maintain component inventory for every application.
- Q** Do you know when vulnerabilities are found in deployed components?
A Monitor component bill of materials for new security flaws and identify applications for critical updates.
- Q** Do you have global visibility into open source usage?
A Know how, when, and where components are consumed organization-wide to identify risks before they become a problem.





Automated Policy Management Throughout the Lifecycle





- Need to recognize that the priorities are different
- Tooling needs to adopt the practice of the practitioner not the other way around
- A Tool is not a process and a process is not a tool learn to leverage both.



Go Fast. Be Secure.

Build security in from the start

Enforce policy in the tools you already use

Reduce risk by automating governance throughout the lifecycle

Reduce cost by fixing early in the process

React to new threats by knowing what they are and where to fix them

Go fast by using tools your developers already know



Thank You!