ARE WE REALLY SECURING OUR APPLICATIONS?

Open Source Software Usage Has

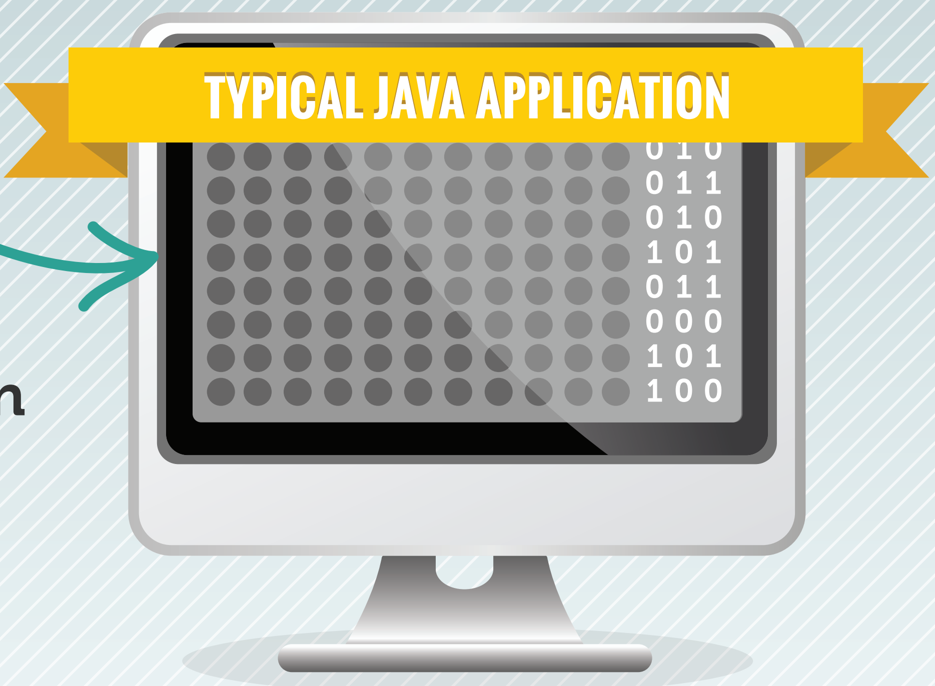
Exploded

2012: 8 Billion

2013: 12 Billion!

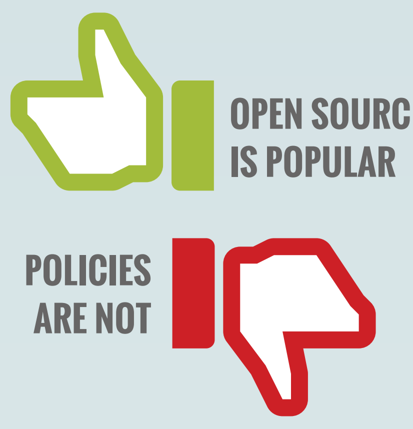
Forever **changing** the way we develop software...

These days, **80%** of an application is assembled from open source components.



Yet only **57%** of organizations have policies governing component usage.

Psssst: and **29%** of those policies don't even address security



71% of all applications contain a critical flaw in at least one open source component

Using risky components is now #9 on OWASP's Top 10 Application Security Concerns.

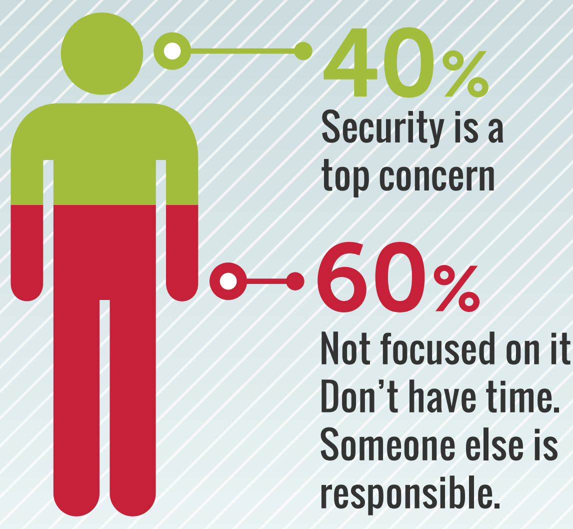
And, nearly **2/3** of organizations don't know which components are used in their applications.

In manufacturing we call this a "Bill of Materials"

Plus, most application security methods can't see components.

Today's popular application "scanning" tools don't assess components (or their dependencies)

60% of developers are not concerned about security



40% Security is a top concern

60% Not focused on it. Don't have time. Someone else is responsible.

CONCLUSION:

We are NOT effectively securing our applications

Top 5 Ingredients to secure apps composed with open source:

1. Application "Bill of Materials" -- you need to know what's in your apps.
2. Automated OSS governance -- manual processes just don't work!
3. Developer control -- provide information within the IDE to make it easy for developers to pick the best components from the start.
4. Governance across the software lifecycle -- policies that are enforced across the DevOps toolchain ensure defense-in-depth.
5. Continuous monitoring -- new vulnerabilities are always being discovered, you need to know where you are at risk.

White paper: Learn how to minimize risk in open source-based applications.

Sonatype

www.sonatype.com

SOURCE: Sonatype 2013 survey of 3500 developers, architects and managers across all industries, company sizes and geographic regions - making it the largest, most comprehensive survey of its kind. www.sonatype.com/survey2013