2016 STATE OF THE SOFTWARE SUPPLY CHAIN

Sonatype

DOWNLOAD FULL REPORT

WHAT IS THE SOFTWARE SUPPLY CHAIN?

It's the flow of open source components through modern software factories.

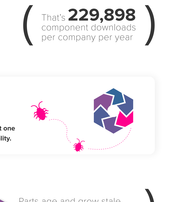
MASSIVE GAINS IN PRODUCTIVITY.

Software Supply Chains allow companies to integrate open source components thus minimizing the amount of code that needs to be developed from scratch

80% to 90% of a typical application is composed of components.

AND THE TREND IS GROWING RAPIDLY.

Use of components has increased 64x over the last 9 years enabling companies to accelerate innovation.



BUT, NOT ALL COMPONENTS ARE CREATED EQUAL.

Companies requested

31 BILLION

of these components last year

That's **229,898** component downloads per company per year

6.8%

of components used in applications have at least one known security vulnerability.

Parts age and grow stale. Older components in apps have **3x rate** of vulnerabilities.

Remediating just

10%

of these defects would cost :

$7.4 MILLION

For an enterprise with 2,000 apps.

THAT'S WHY SMART COMPANIES PRACTICE SOFTWARE SUPPLY CHAIN HYGIENE:

-Build quality in from the beginning.
-Spend less time fixing mistakes.
-Deliver better software faster for less.

GET THE FULL REPORT

sonatype.com/SSC2016

- More insights
- Industry spotlights
- Leading practices

ABOUT SONATYPE'S 2016 STATE OF THE SOFTWARE SUPPLY CHAIN REPORT

As caretakers of the Central Repository, Sonatype services more than 31 billion download requests per year for open source components. We literally feed millions of developers the software parts they require to manufacture and continuously deliver modern applications.

From this unique vantage point, we've amassed a great deal of data and we've developed deep intelligence with respect to the staggering volume and variety of open source components flowing through software supply chains into development environments. In this report, we share information that has been invisible to many in order to make it visible to all.

OUR SOURCES

- Analysis of annual downloads from the Central Repository in calendar year 2014 and 2015. Developer population count courtesy of openhub.net.
New open source projects and version counts analyzed from modulecounts.com.