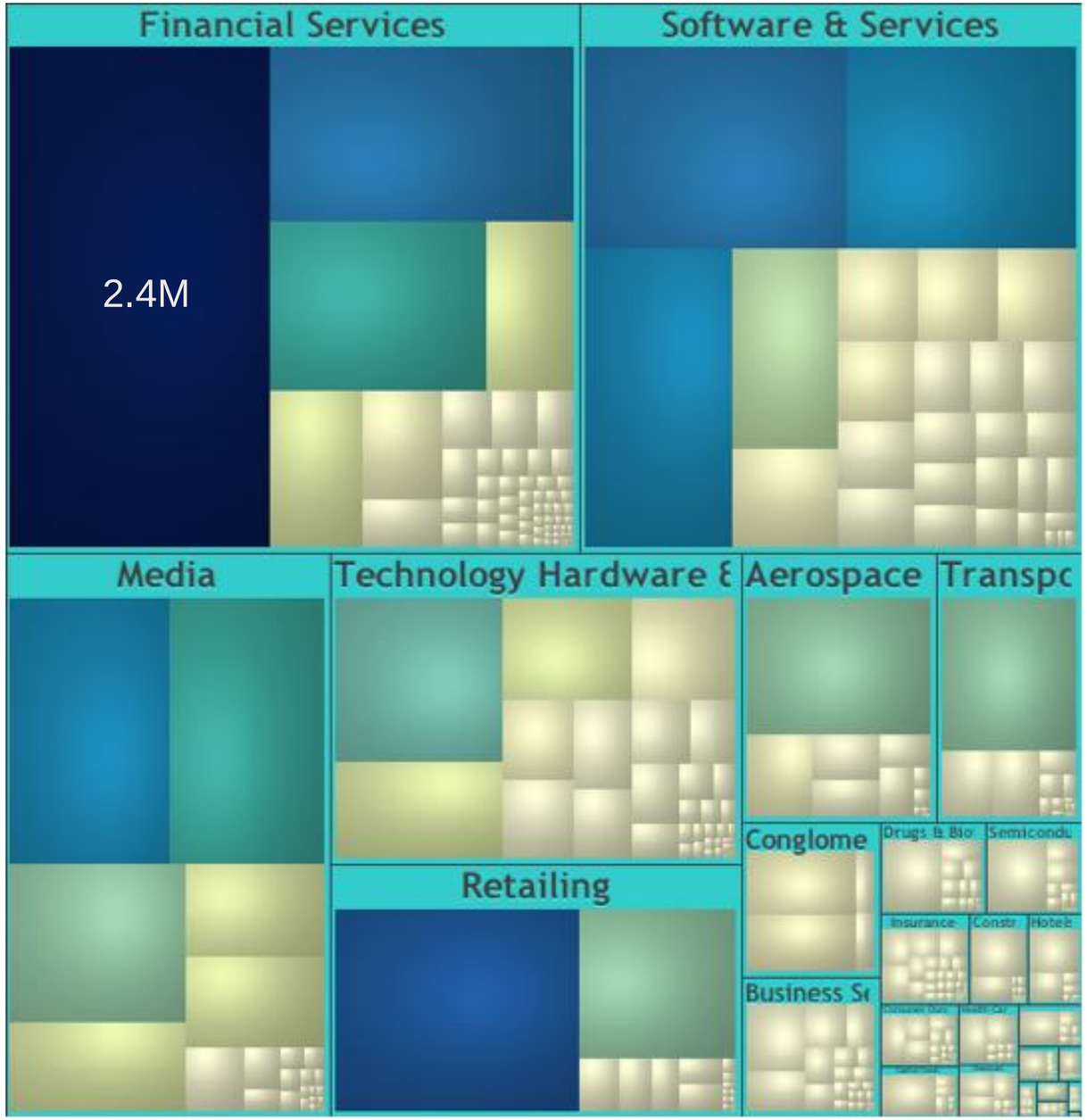
Sonatype

Open Source in Application Development

Governance is a Full Lifecycle Issue

Brian Fox
Vice President, Product Management
Sonatype Inc.
brianf@sonatype.com

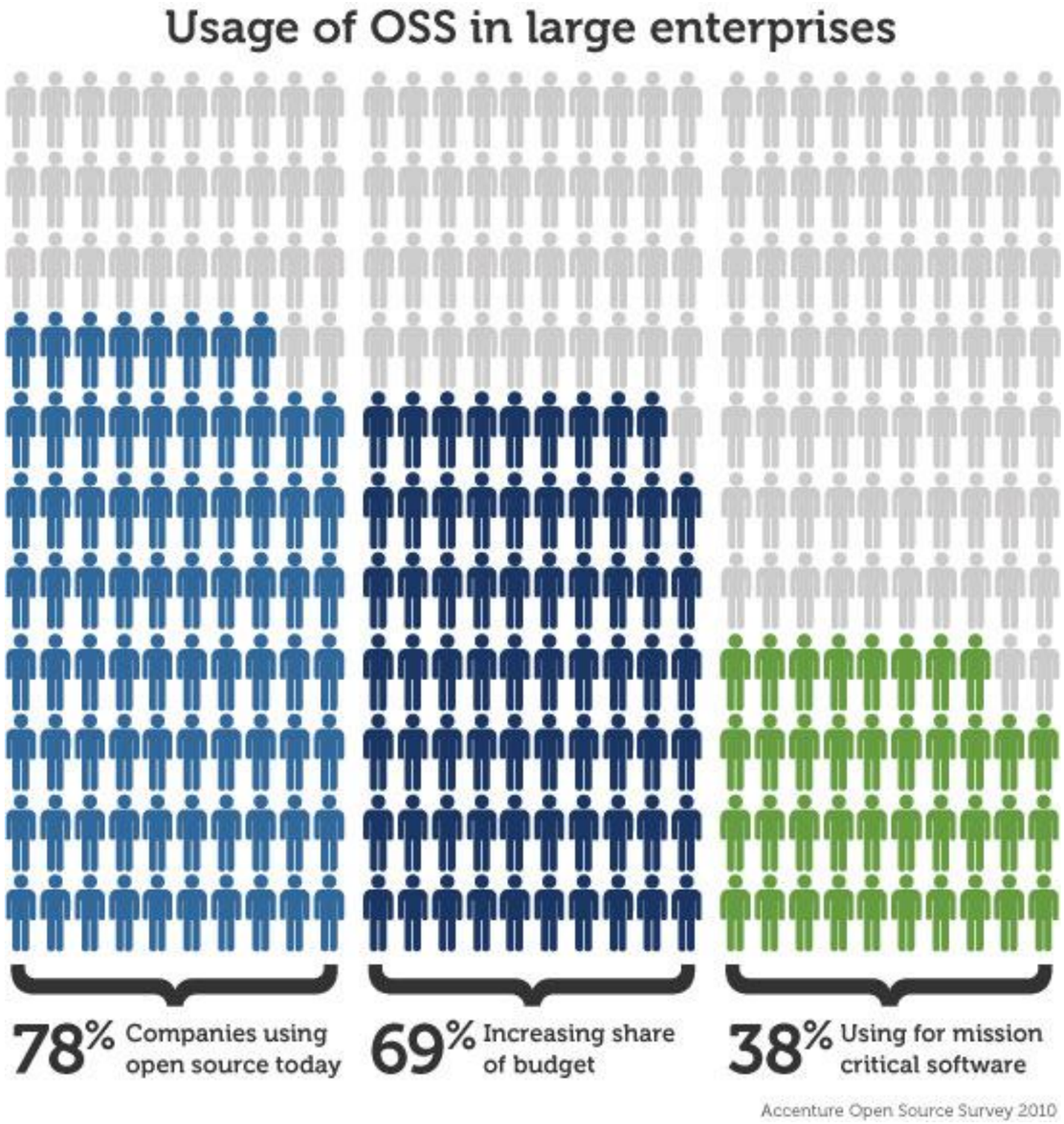


The Global 2000:

Annual Component Downloads

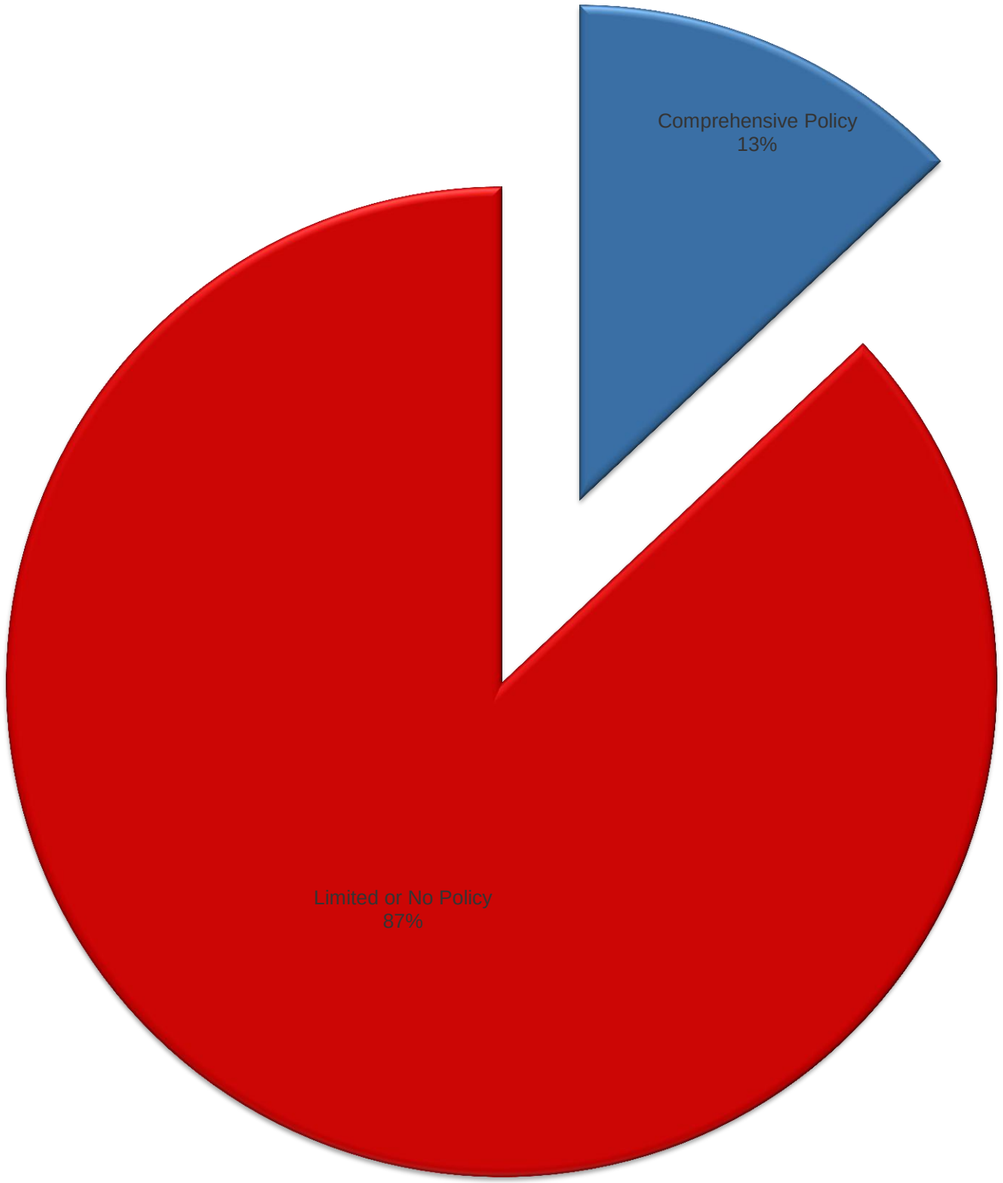
(non-unique)

Usage is Growing

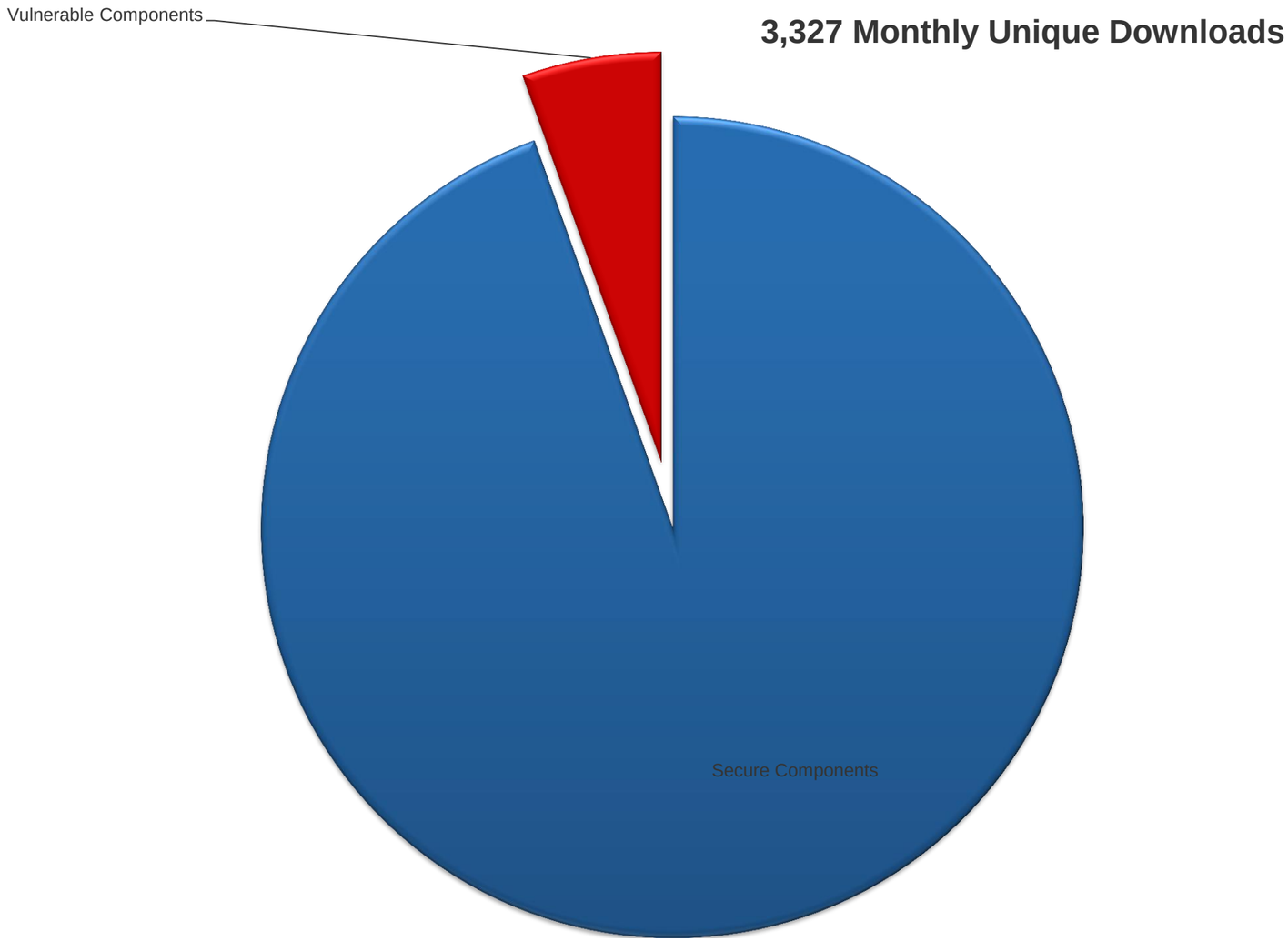


Quality	How do we ensure we're using the best quality components?
Security	How do we know components don't have security vulnerabilities?
License	How do we know components meet our license requirements?

87% Ungoverned

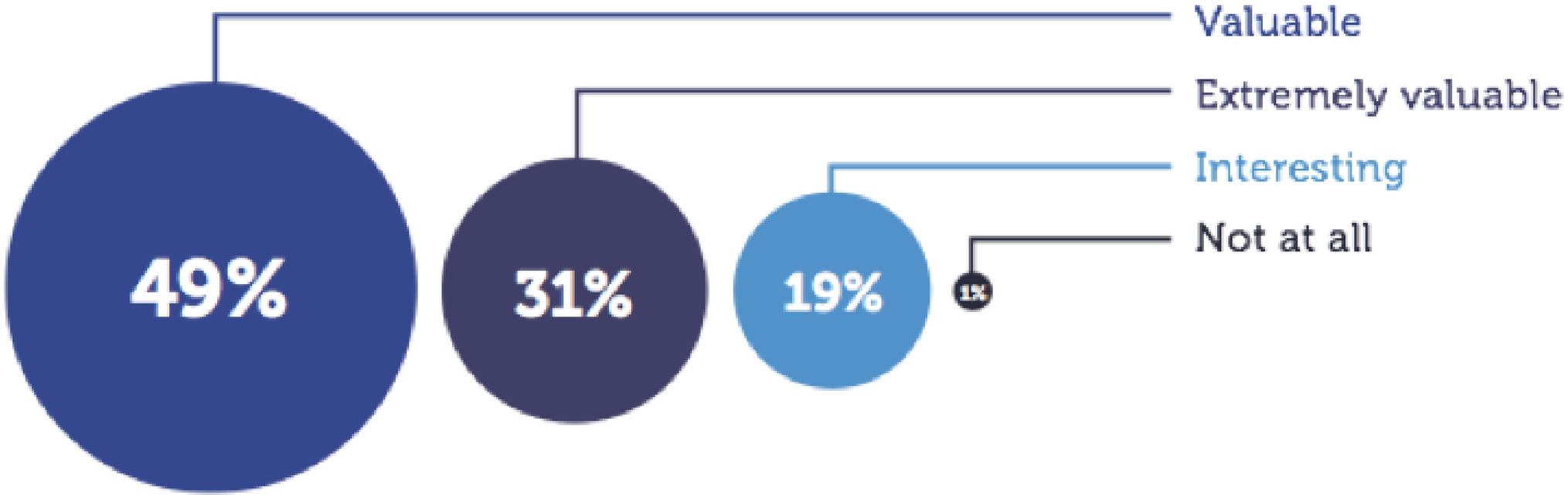


A Global 100 Financial Institution



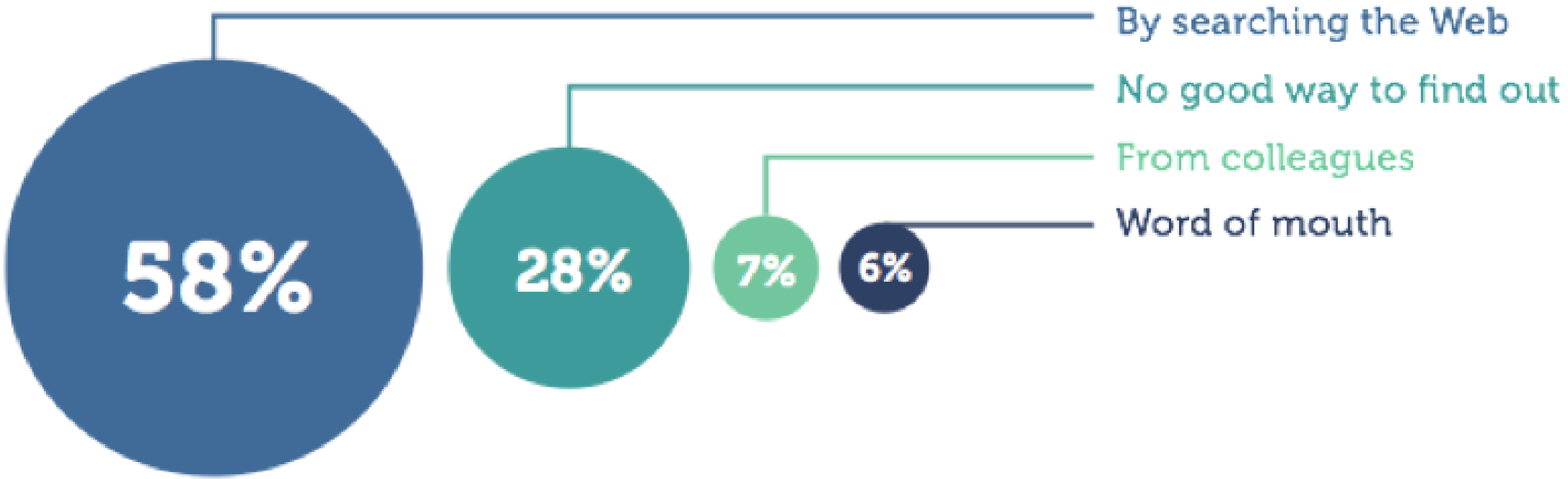
Change Awareness is Considered Valuable

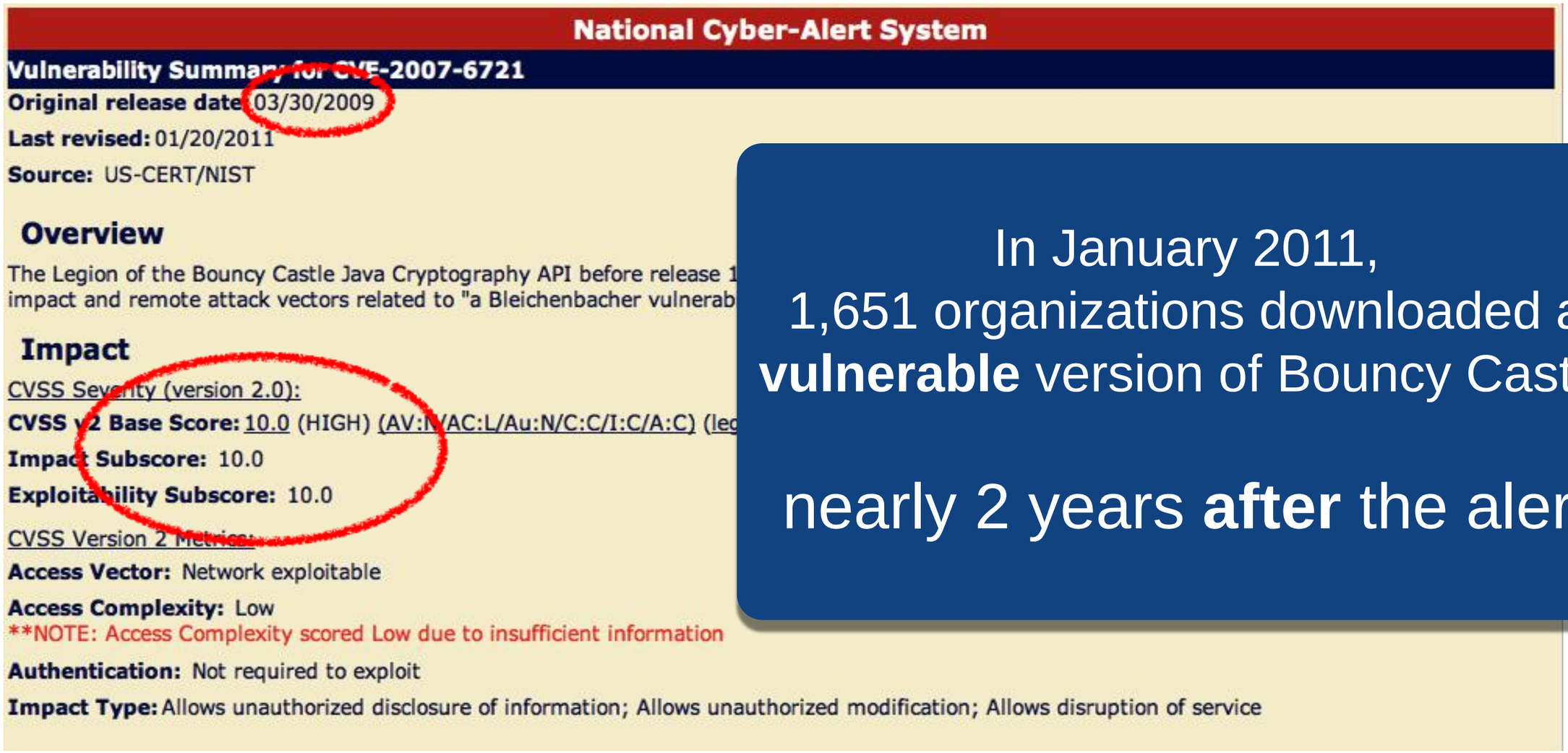
Would you like immediate notification of changes?



Change Awareness is a Tremendous Challenge

When an artifact changes, how do you know?





National Cyber-Alert System

Vulnerability Summary for CVE-2007-6721

Original release date: 03/30/2009

Last revised: 01/20/2011

Source: US-CERT/NIST

Overview

The Legion of the Bouncy Castle Java Cryptography API before release 1
impact and remote attack vectors related to "a Bleichenbacher vulnerab

Impact

CVSS Severity (version 2.0):

CVSS v2 Base Score: 10.0 (HIGH) (AV:N/AC:L/Au:N/C:C/I:C/A:C) (leg

Impact Subscore: 10.0

Exploitability Subscore: 10.0

CVSS Version 2 Metrics:

Access Vector: Network exploitable

Access Complexity: Low

**NOTE: Access Complexity scored Low due to insufficient information

Authentication: Not required to exploit

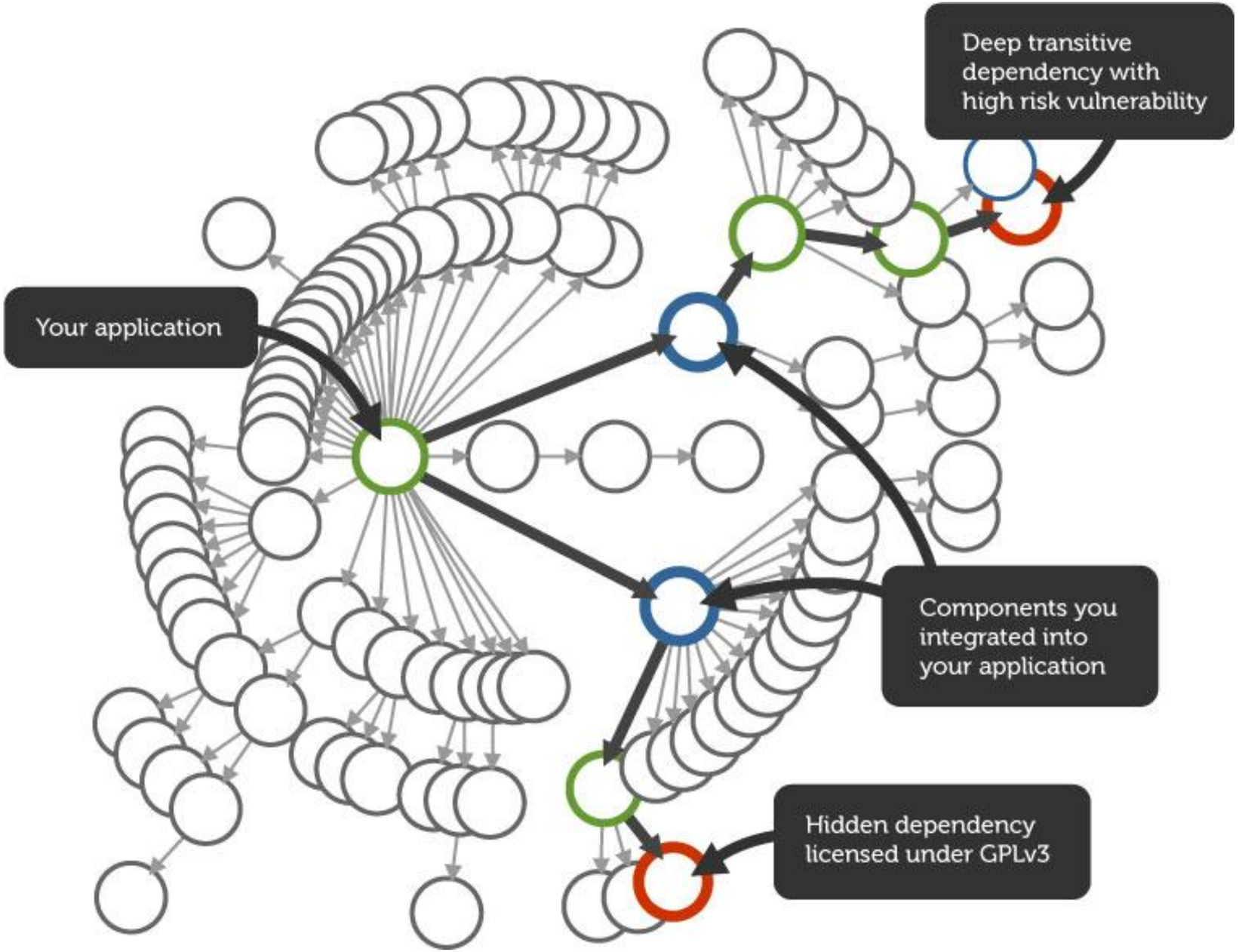
Impact Type: Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service

In January 2011,
1,651 organizations downloaded a
vulnerable version of Bouncy Castle

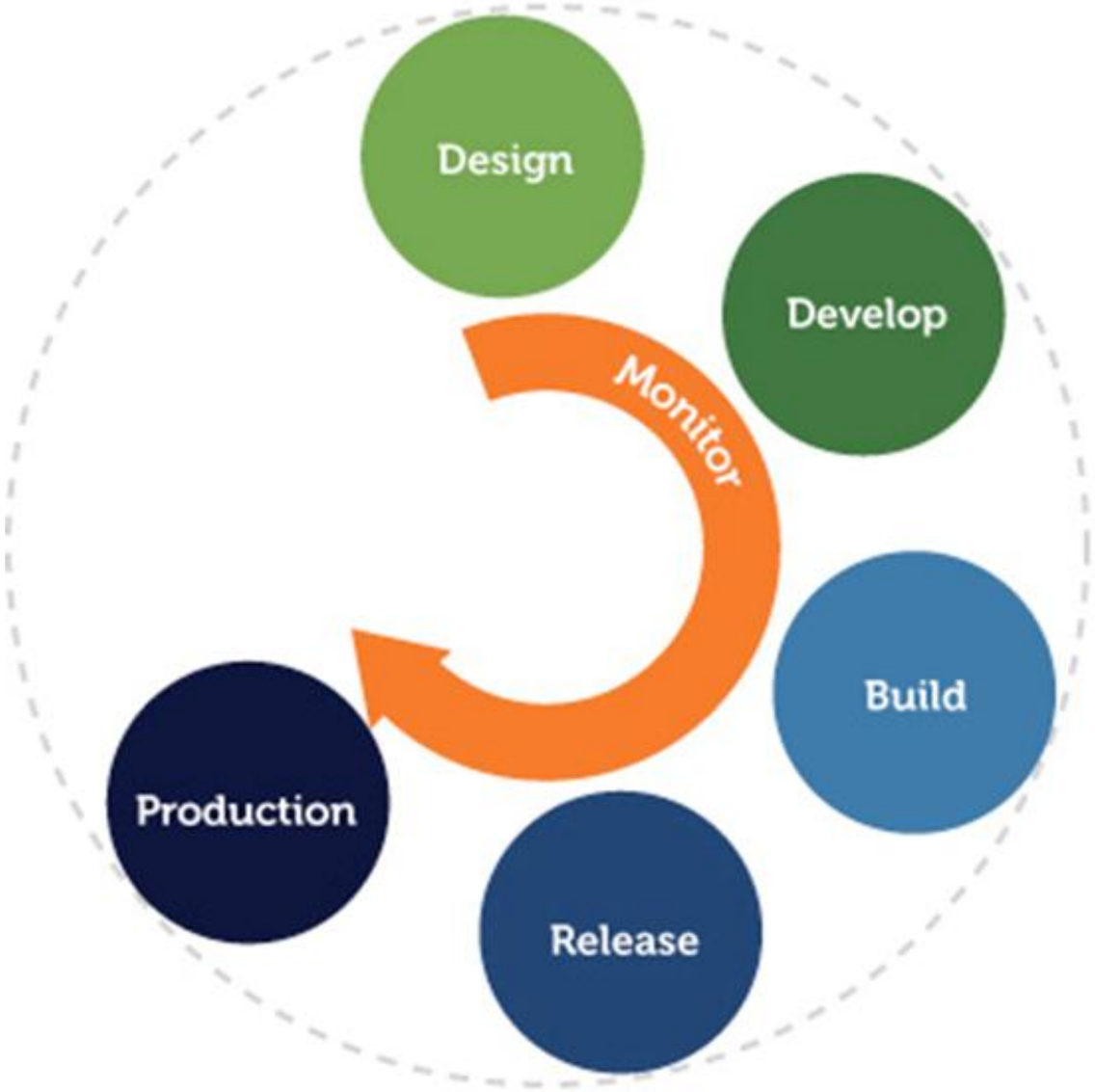
nearly 2 years **after** the alert

** Source: National Vulnerability Database Version 2.2. Sponsored by DHS National Cyber Security Division*

The Challenge of Transitive Dependencies



Open Source Management is a Full Lifecycle Issue



- Develop Governance policy with the App Dev org:
  - Eliminate/Avoid defects early
  - Leverage tooling across entire lifecycle
  - Enforce policy at multiple checkpoints
  - Monitor “inventory” continuously

Sonatype

Open Source in Application Development

Governance is a Full Lifecycle Issue

Brian Fox
Vice President, Product Management
Sonatype Inc.
brianf@sonatype.com