Managing Open Source-Associated Risk

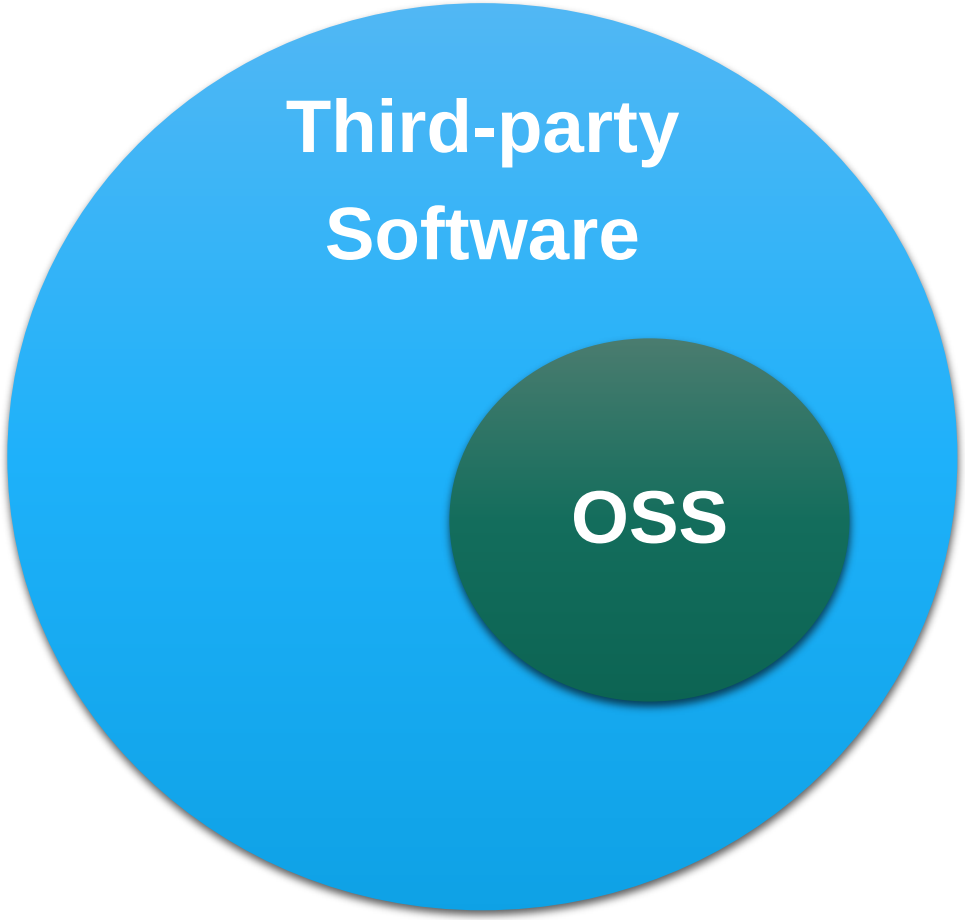
Matthew H. Jacobs, Vice President & General Counsel
Black Duck Software, Inc.

BLACKDUCK

What is Open Source Software (OSS)?

Binary v. Source

It’s third party software



BLACKDUCK

The OSS Universe is Ever Expanding

530

Number of lines of open source code (Billions)

(10 Million+ developer years)

2500

Number of different open source licenses

9000

Number of open source forges and repositories

79000

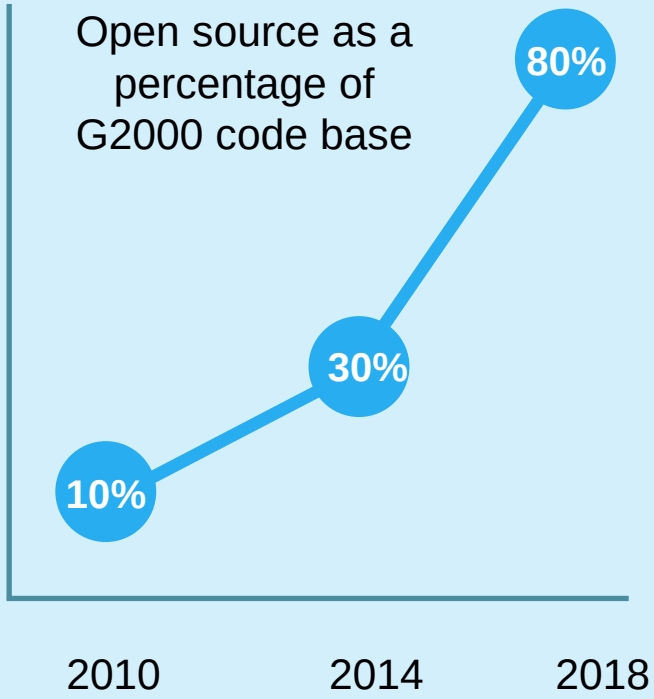
Number of known OSS vulnerabilities

BLACKDUCK

OSS Has Passed the Tipping Point

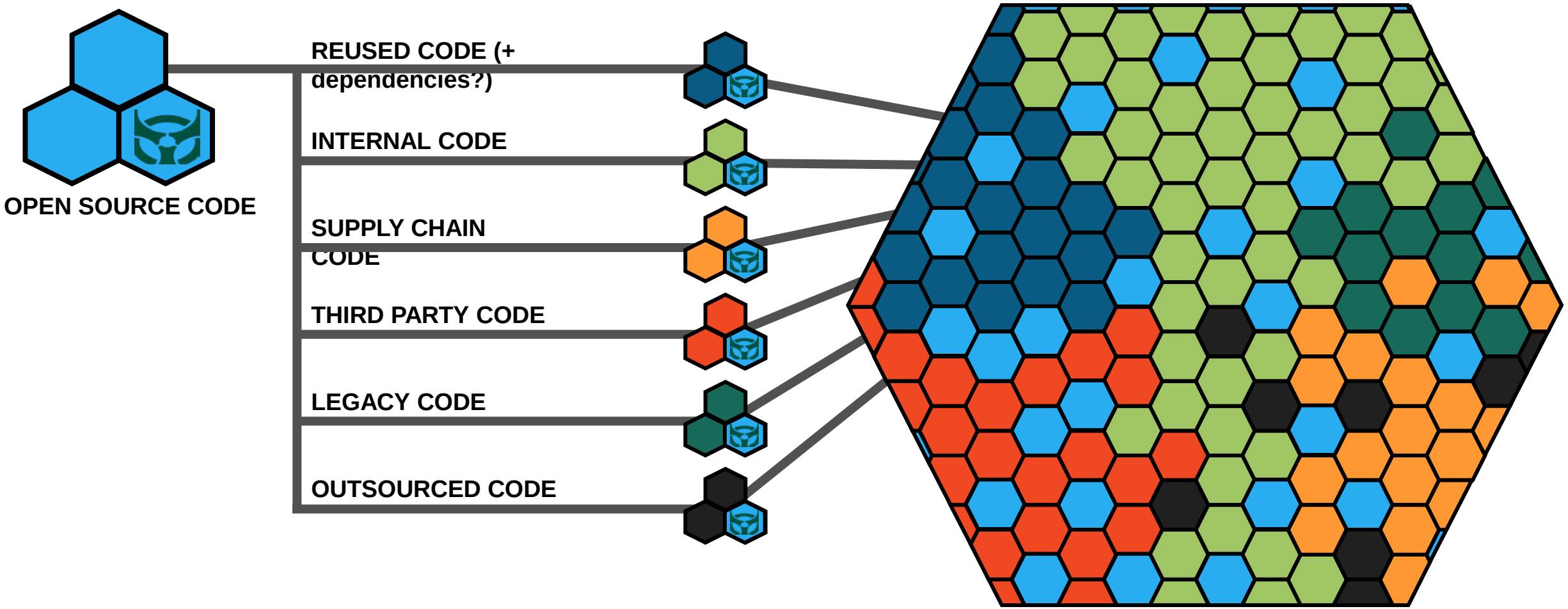
Of organizations will face problems because of a lack of open source policy.

Source: Gartner



BLACKDUCK

Open Source Enters the Code Base in Many Ways



BLACKDUCK

Primary OSS License Categories

- Permissive Licenses
  - Licensee can use, copy, modify and distribute the software.
  - Licensee is allowed to combine the source with open source or proprietary software.
  - Licensee is NOT obligated to distribute the source code of derivative works.

- Copyleft Licenses
  - Any Licensee modifications to the software (derivative works) must be, if distributed, distributed under the same reciprocal license.
  - Copyleft licenses are substantially more complex than permissive licenses.

- BSD
- MIT

- GPL

BLACKDUCK

GPL and the SAAS Loophole: Is SAAS a Distribution?

GPL v2

Frequently Asked Questions

A company is running a modified version of a GPL'ed program on a web site. Does the GPL say they must release their modified sources?

The GPL permits anyone to make a modified version and use it without ever distributing it to others. What this company is doing is a special case of that. Therefore, the company does not have to release the modified sources.

GPL v3

Section 0

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. ***Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying****.*

AGPL v3

Section 13

Notwithstanding any other provision of this License, if you modify the Program, your modified version ***must prominently offer all users interacting with it remotely through a computer network … an opportunity to receive the Corresponding Source of your version*** *by providing access to the Corresponding Source from a network server at no charge, through some standard or customary means of facilitating copying of software.*

Key Points

- AGPL v3 largely replicates the terms of the GPL v3.
- Includes extra provision on "Remote Network Interaction". Intended to close loophole.
- Does not affect intranets and internal networks.

BLACKDUCK

Many fringe licenses

- Beer-ware

- WTF!

- Fender Stratocaster

- No-nuke

- Chicken Dance

BLACKDUCK

Who’s Responsible for Security?

Commercial Code

- Dedicated security researchers
- Alerting and notification infrastructure
- Regular patch updates
- Dedicated support team with SLA

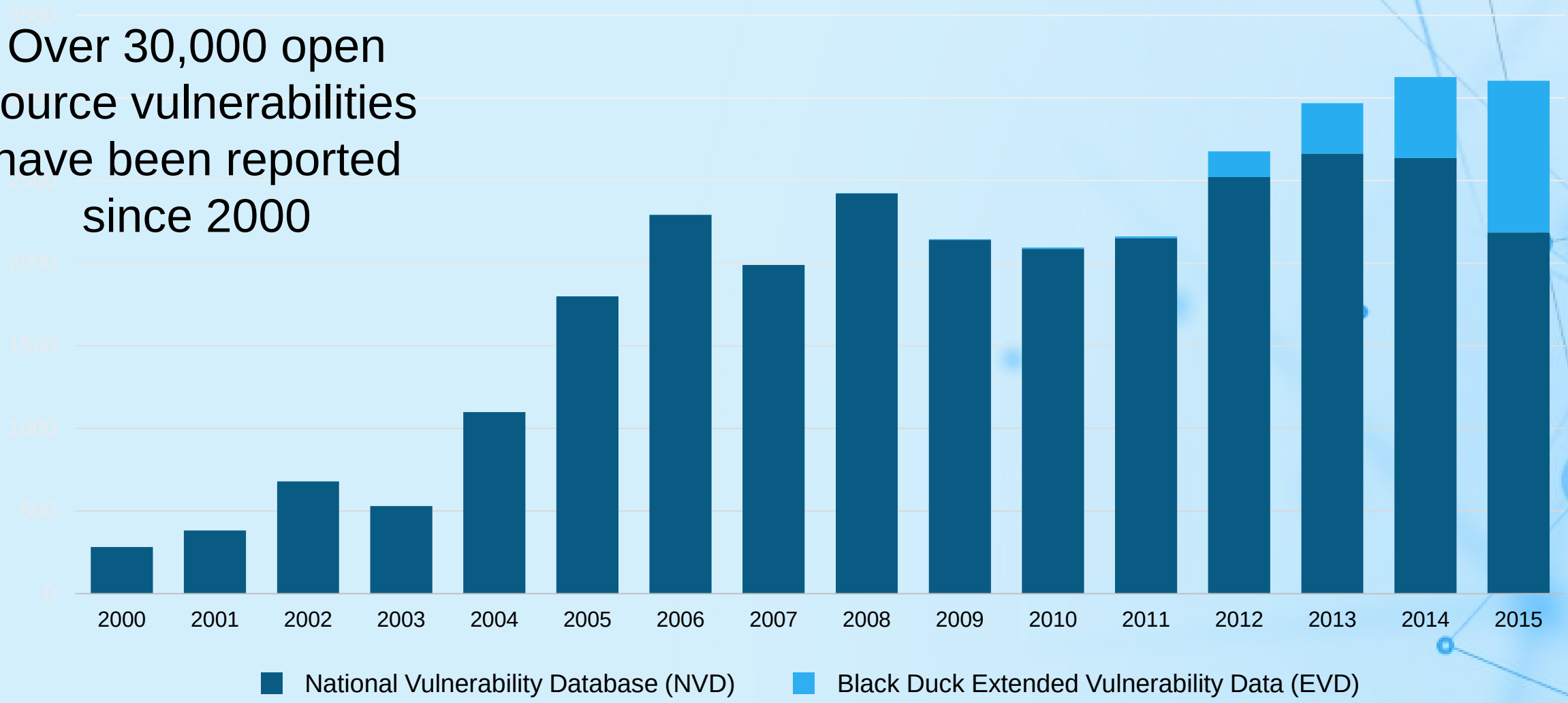
Open Source Code

- Community based code analysis
- Monitor newsfeeds yourself
- No standard patching mechanism
- Ultimately, you’re responsible

BLACKDUCK

Number of Vulnerabilities Increasing

Over 30,000 open source vulnerabilities have been reported since 2000



BLACKDUCK

What do These Vulnerabilities Have in Common?

Ghost
Since: 2000
Discovered: 2015
Component: GNU C Library
Discovered By: Qualys researchers

Shellshock
Since: 1989
Discovered: 2014
Component: Bash
Discovered By: Chazelas

Heartbleed
Since: 2011
Discovered: 2014
Component: OpenSSL
Discovered By: Riku, Antti, Matti

Venom
Since: 2004
Discovered: 2015
Component: QEMU
Discovered By: Geffner

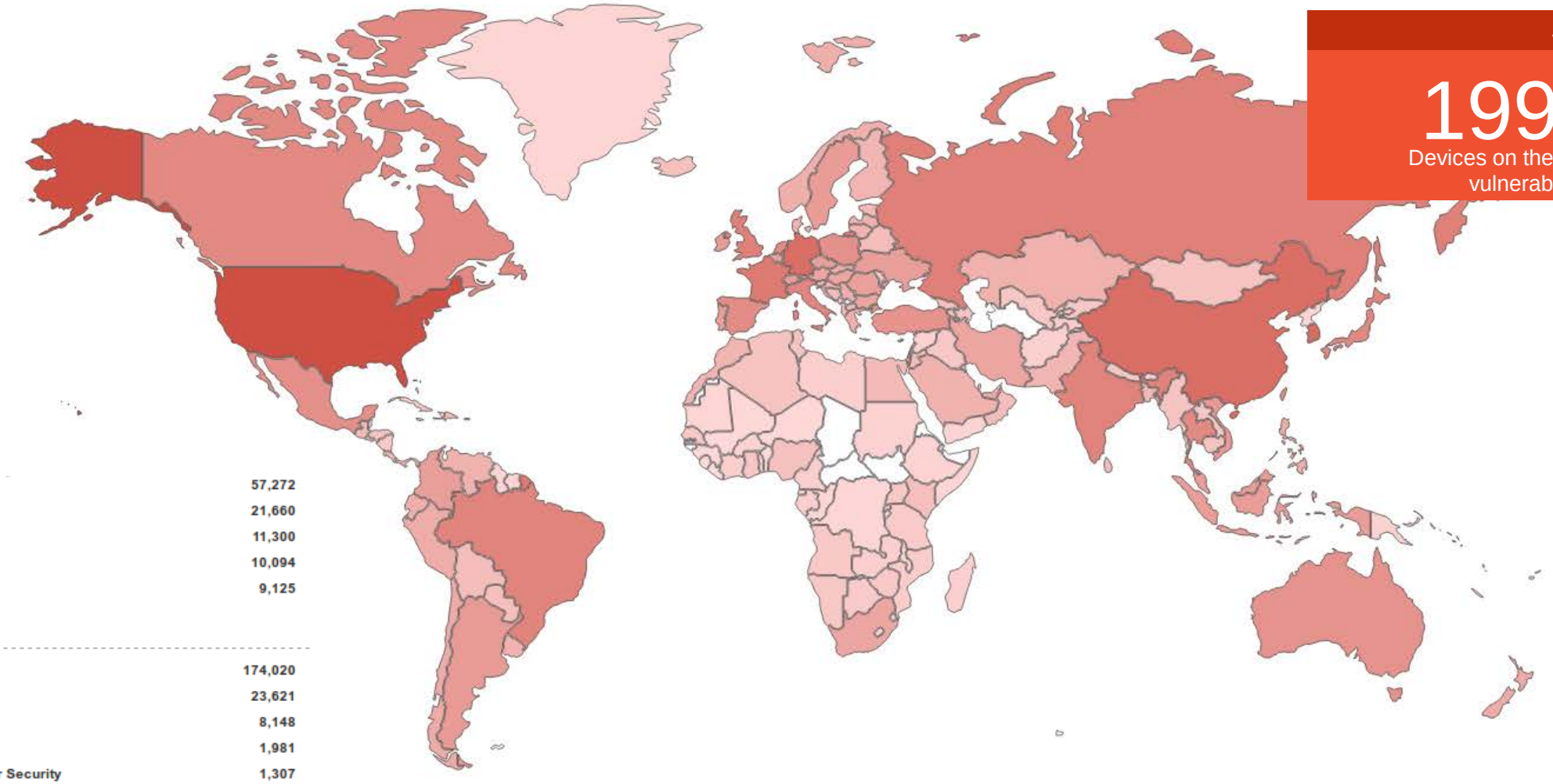
BLACKDUCK

Heartbleed is Still a Threat

January 2017

199594

Devices on the internet are still vulnerable to Heartbleed



United States	57,272
Germany	21,660
China	11,300
France	10,094
United Kingdom	9,125

TOP SERVICES

HTTPS	174,020
HTTPS (8443)	23,621
Webmin	8,148
8081	1,981
Symantec Data Center Security	1,307

BLACKDUCK

What if the Automotive Market Treated Recalls Like Open Source Users Treat Vulnerabilities?

Known and Quantified

Continental Airbag Recall Affects 5 Million Vehicles

Posted on 05 February 2016 by Nicole Wakelin

Facebook Twitter Reddit This

Continental Automotive Systems Inc. issued a recall affecting 5 million vehicles worldwide due to possibly faulty airbag control unit. The National Highway Traffic Safety Administration received word that a power supply component in the airbag might corrode

Known and Unquantified

siliconANGLE Cloud Mobile Social Big Data Bleedi

OpenSSL Heartbleed vulnerability may affect millions

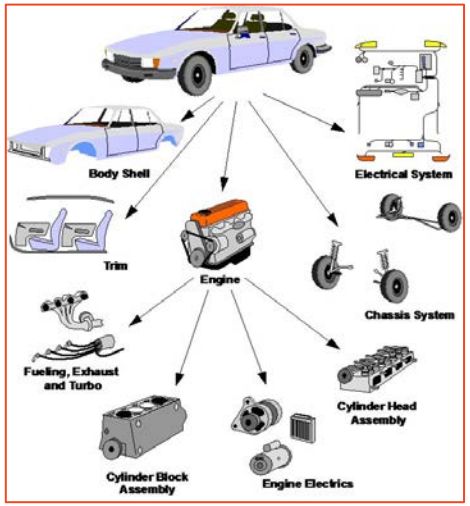
by John Casaretto | Apr 8, 2014 |

In IT circles, the phrase 'bleeding heart' may never mean what it used to as **heartbleed** news of this extremely serious **Heartbleed vulnerability** is traveling fast. The vulnerability was recently found in Open SSL, the most popular library used to secure the internet in widely used distributions. OpenSSL is an open source implementation of the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols by which much of web security is implemented. The bug allows for anyone on the internet to read the memory of the systems running the affected versions of OpenSSL. With this ability, the secret keys utilized by SSL/TLS encryption can be stolen. That means massive compromises could be in store for virtual private networks (VPNs), email, web pages, instant messaging (IM), and passwords. Given the gravity of the vulnerability, reports that **bitcoin services had been affected** are but one of the potential targets that are likely to emerge as having been affected by this massive bug. This has potential impact for all web services from throughout the web.

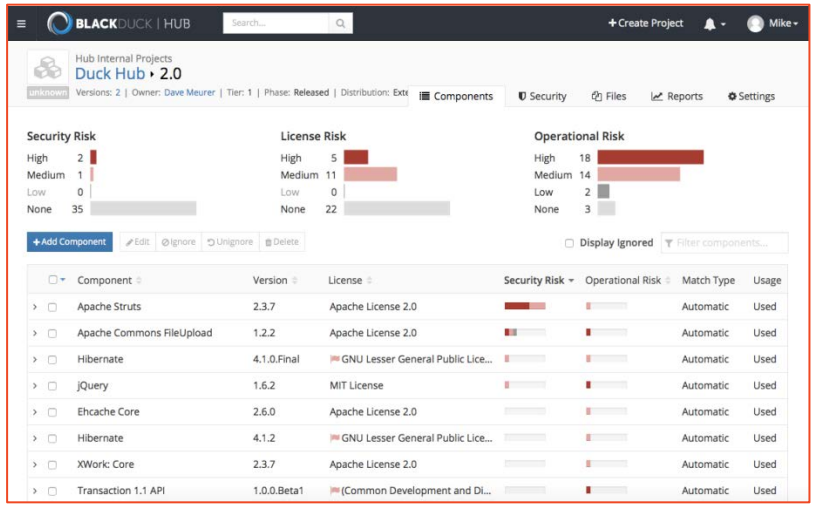
The versions of OpenSSL that are affected, version 1.0.1 and 1.02-beta release have been widely deployed for some time. The bug has been described as a program error, and a fix has been published for the 1.01 program in OpenSSL 1.01g. The bug was found in the heartbeat extension (RFC6520) of the Transport Layer Security/Datagram Transport Layer Security (TLS/DTLS) within the implementation on the affected OpenSSL versions. It is a straight, pure bug that unfortunately strikes at the 'heart' of web security, affecting that heartbeat extension, thus earning its name. According to security reports, research has produced some significant leaks. In testing, attacks were able to be executed without leaving a trace. The tests were also able to steal X.509 certificates, user names and passwords, instant messages, emails and business critical documents and communication – all without any privileged information or any credentials.

BLACKDUCK

A Software Bill of Materials Solves the Problem



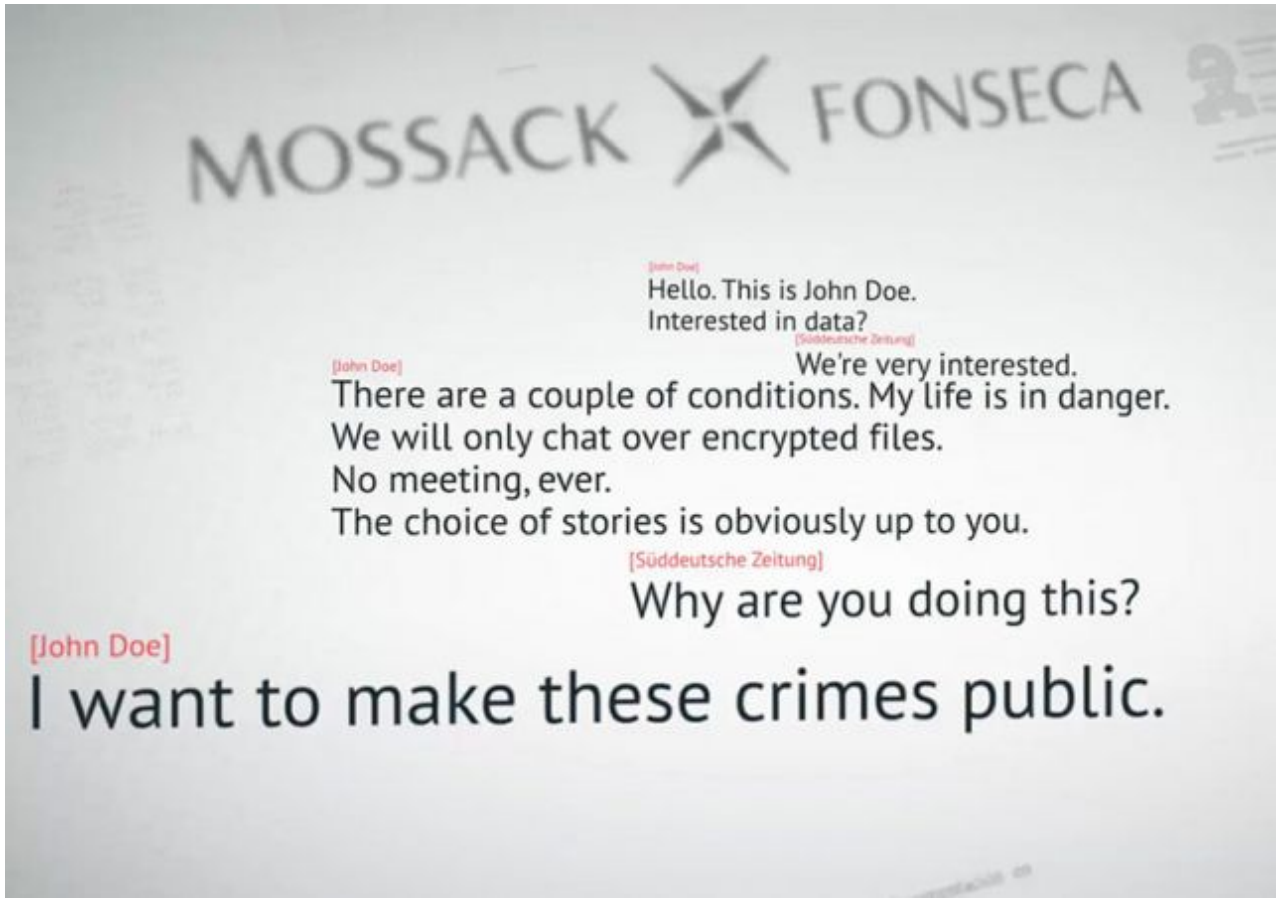
- Components and serial numbers
- Unique to each vehicle VIN



- Complete analysis of open source components
- Unique to each project or application
- Security, license, and operational risk surfaced

BLACKDUCK

Open source security is a serious legal risk



2.6 TB data
11.5M documents
214,000 accounts
140 politicians and public officials

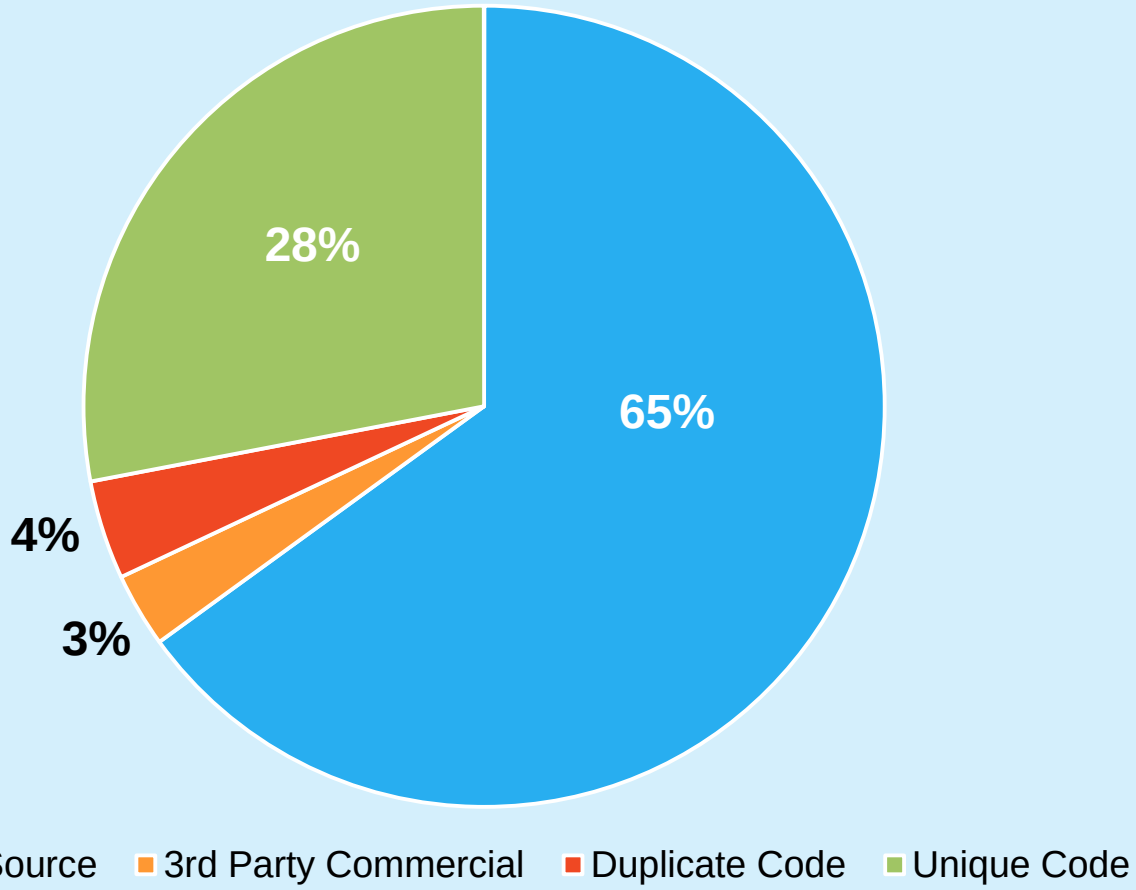
Drupal
- 2 years old
- > 25 vulns

WordPress
- 3 months old
- has known vulns

VULNERABILITIES LEAD TO BREACHES WHICH LEAD TO LAWSUITS

BLACKDUCK

Open Source Adoption in Enterprise



A typical enterprise IT organization has thousands of applications and uses hundreds of open source components.

Enterprise Average: 30% open source in an application

BLACKDUCK

Black Duck's Experience Analyzing Code

- 99% of code audits find open source.
- 95% of audits find unknown open source.
- 50% of code audits contain GPL.
- Audits on average contain 33% open source.
- 67% of audits find open source with known security vulnerabilities.

BLACKDUCK

Overall Impacts on the Deal

Macro Impacts:

- **Delay**
  - Signing
  - Closing
- **Reduce Price**
  - By expected cost of remediation
  - By estimate of past non-compliance
  - Plus a premium for the unknown
- **Deal certainty**
  - Due to conditions
  - Dependence on third parties
- **Kill the deal**
  - Upset the build vs. buy decision

Diligence/Scheduling Impacts:

- **Inability to provide basic materials requested in diligence and for schedules**
  - List of in-licensed software with license and usage for each item
  - Open source policy
- **Surprises discovered during diligence**
- **Inability to cleanly make reps**

Lead to Additional:

- **Diligence, such as a code scan**
- Reps and warranties
- Remediation covenants and closing conditions
- Specific indemnities
- Escrows

BLACKDUCK

Why Should You Care About This?:

Shifting landscape of open source license enforcement

- If you don't care, your customers, lenders, underwriters, regulators, investors, acquirers will.
- Trolls! Patrick McHardy
- No longer brought for ideological reasons; now commercial software companies on both sides with hundreds of millions at risk. Recent litigation:

	Artifex Software v. Hancom	CoKinetic Systems v. Panasonic Aviation
Filed	December 2016	March 2017
Claims	GPL violations, copyright infringement, etc. (dual licensing)	Anticompetitive refusal to distribute source code, breach of the GPL v2. ("intended third-party beneficiary")
Alleged Damages	"All gains, profits and advantages"	Specific performance, public disclosure of Panasonic source code

FTC Guidance – June 2015

START WITH SECURITY

A GUIDE FOR BUSINESS

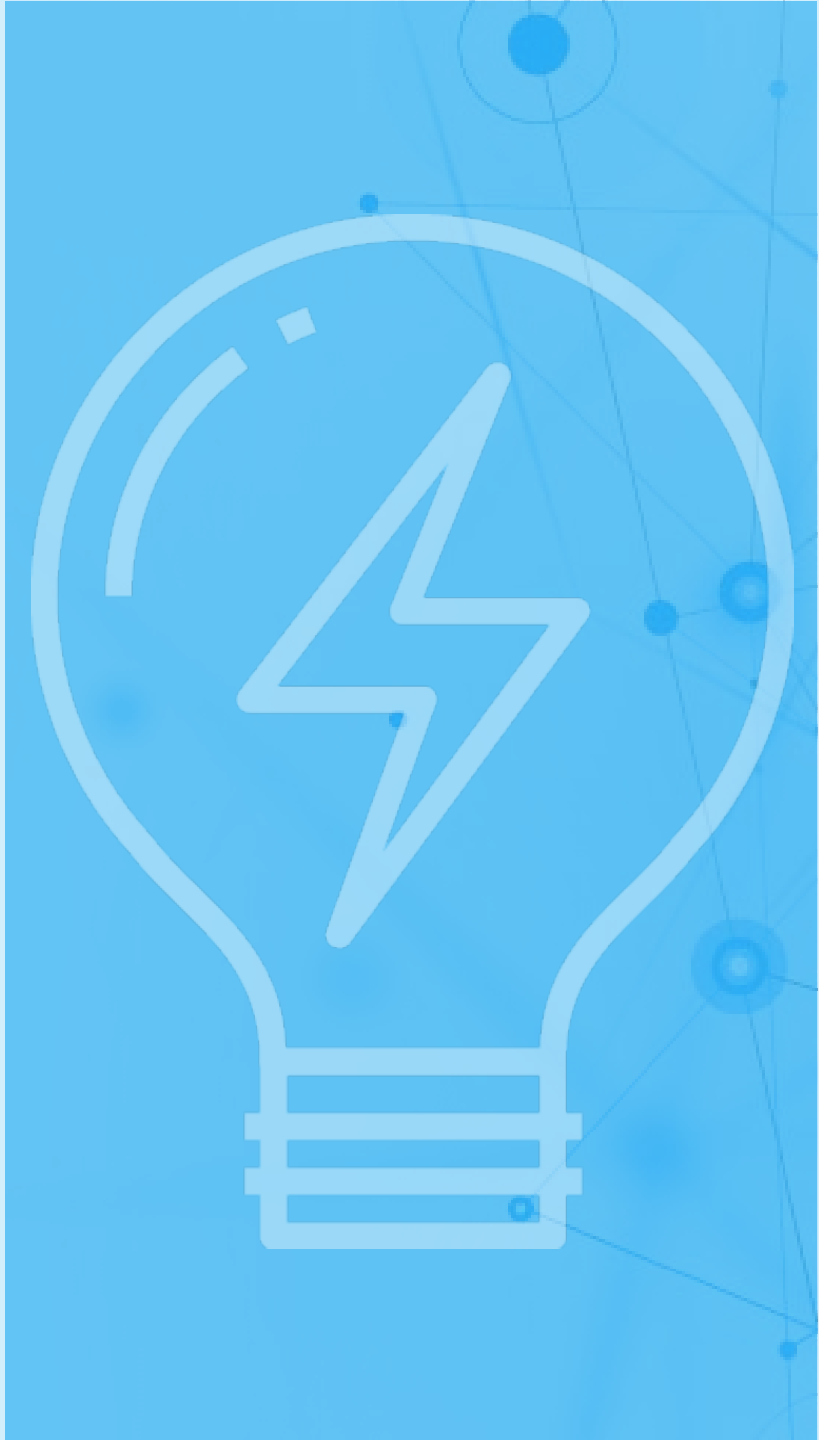
LESSONS LEARNED FROM FTC CASES

BLACKDUCK

Start with SECURITY: 10 FTC Lessons from 50+ FTC Data Security Settlements

1. Start with security.
2. Control access to data sensibly.
3. Require secure passwords and authentication.
4. Store sensitive personal information securely and protect it during transmission.
5. Segment your network and monitor who’s trying to get in and out.
6. Secure remote access to your network.
7. **Apply sound security practices when developing new products**.
8. **Make sure your service providers implement reasonable security measures**.
9. **Put procedures in place to keep your security current and address vulnerabilities that may arise**.
10. Secure paper, physical media, and devices.

BLACKDUCK



Keeping watch….

INVENTORY

Open Source Software

MAP

Known Security Vulnerabilities

IDENTIFY

License Compliance Risks

TRACK

Remediation Priorities & Progress

ALERT

New Vulnerabilities Affecting You

BLACKDUCK

BLACKDUCK