GDPR & OPEN SOURCE SECURITY BY THE NUMBERS

You can't protect what you don't know about. Talk to your heads of software development and information security and ask them to produce a list of open source components your organization uses. Here's why you need to know.

• May 2018 •

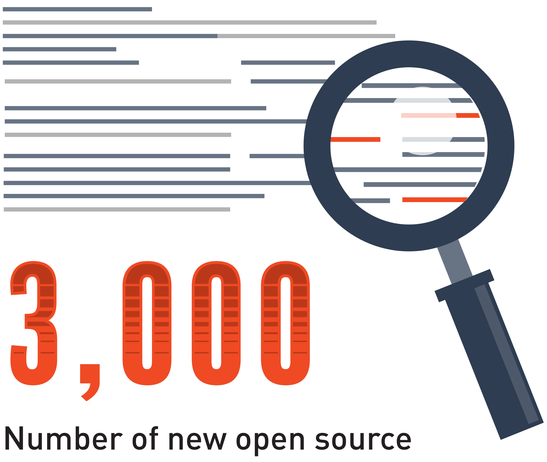
25

5/25/2018

Date the responsibility of protecting any personal data you hold or process on EU citizens will fall squarely on the shoulders of your organization.

147 | 27

Software applications include an average 147 unique open source components. Each application contains, on average, 27 vulnerable open source components.



3,000

Number of new open source vulnerabilities identified yearly.

25 | 32 | 35

Three key GDPR Articles mandating that organizations must demonstrate observance of the GDPR, including "appropriate measures" for security. But many companies aren't including open source security in their plans.

€20M | 4%

Breaches could lead to fines of up to €20 million or 4% of global annual turnover. A single violation could put your company out of business.

£100,000

A fine recently levied against a public agency over its failure to fix an open source software security hole in its website. The vulnerability was exploited by a hacker who accessed sensitive employee personal data.

BLACKDUCK BY SYNOPSYS

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in static analysis, software composition analysis, and application security testing, is uniquely positioned to apply best practices across proprietary code, open source, and the runtime environment. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations maximize security and quality in DevSecOps and throughout the software development life cycle.

For more information go to www.synopsys.com/software.