SYNOPSYS®

GDPR and Open Source Security Management

The EU General Data Protection Regulation (GDPR) mandates that all companies processing and/or holding the personal data of EU residents must protect that information—regardless of where it is sent, processed, or stored.

Any organization either based in the EU or that processes or holds the personal data of European residents will need to adhere to GDPR when it goes into effect in 2018. Failure to do so could mean heavy penalties—fines up to 4% of annual global revenue or up to €20 million (approximately US$22.3 million), whichever figure is higher.

A challenge and opportunity for your business

Organizations newly defined as "processors" of their customers' data can turn this classification to their advantage by differentiating themselves and opening new business opportunities for their firms. Many customer companies will require their vendors to observe GDPR as part of the RFP process and/or privacy and security audits. Failure to do so could lead to significant loss of business to competitors who can demonstrate their GDPR observance.

Is my company impacted by GDPR?

- Does my company offer goods or services to EU residents?
- Does my company monitor, collect, or process personal data of EU residents?
- Does my company have employees in the EU?

If you answered yes to any of those questions, you must observe GDPR regulations.

Application security and GDPR

From an application security standpoint, the key element of GDPR is Article 32, "Security of processing." Both those controlling personal data and those processing that data must take "appropriate technical and organisational measures to ensure a level of security appropriate to the risk," including establishing processes for regularly assessing and testing their security practices.

Where open source security management fits in

Today's software is built on a core of open source. Why spend time and money reinventing the wheel when freely available open source software components already exist? That's why you'll find open source code in over 90% of today's software applications.

But many organizations don't pay sufficient attention to the security exposures created by vulnerable open source components, and they may not even be aware these exposures exist. In Synopsys' most recent analysis of more than 1,000 commercial applications examined by the Black Duck audit services group, known open source vulnerabilities were found in over 65% of those applications.

For example, OpenSSL was among the most common high-risk components found by the Black Duck audits. OpenSSL, an open source project contained in hundreds of thousands of applications that need to secure communications over computer networks against eavesdropping, is used by many businesses for their websites, email and chat servers, and client-side software.

Heartbleed, a critical security flaw of OpenSSL that can expose supposedly secure communications, was first used in 2014 to steal personal taxpayer data from the Canada Revenue Agency. Yet years later, many companies still use a version of OpenSSL containing the Heartbleed vulnerability owing to a lack of insight into their open source use, opening themselves to possible data breaches and GDPR fines. Thousands of similar vulnerabilities—some less dangerous than Heartbleed, some even more so—exist in many open source components today.

How Synopsys can help

Every organization affected by GDPR needs a comprehensive approach to open source security management as it pertains to GDPR observance. Our solutions enable open source management best practices that allow organizations to know the open source in their code, reduce risks, tighten policies, and monitor and audit for compliance and policy violations.

Black Duck software composition analysis automates identification of all open source in use, giving you visibility into any known open source security vulnerabilities as well as compliance issues. With Black Duck, you can define and enforce open source use and risk policies, while continuously monitoring for new vulnerabilities.

Black Duck software audits are recognized as the industry standard where there is a need to quickly and completely inventory open source software, identifying open source security issues in applications as well as code quality and potential IP risks.

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 application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations optimize security and quality in DevSecOps and throughout the software development life cycle.

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

Synopsys, Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

Contact us:
U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com