SYNOPSYS®

CASE STUDY

ScienceLogic

ScienceLogic Gains Unmatched Visibility Into Open Source With Black Duck

Company overview

ScienceLogic is a leader in IT Operations Management, providing modern IT operations with actionable insights to predict and resolve problems faster in a digital, ephemeral world. Trusted by thousands of organizations, ScienceLogic's technology was designed for the rigorous security requirements of United States Department of Defense, proven for scale by the world's largest service providers, and optimized for the needs of large enterprises.

"How much would it cost to ensure there are no license compliance or security issues if we weren't monitoring open source with Black Duck?"

Overview

Founded in 2003, ScienceLogic simplifies datacenter, cloud, system, and network monitoring with their all-in-one IT operations. Over 25,000 global service providers, enterprises, and government organizations rely on ScienceLogic every day to enhance their IT operations. With ScienceLogic's platform, customers can maximize efficiency, optimize operations, and ensure business continuity.

The challenge: Ensuring open source security and license compliance

"We have a number of open source packages that we use within the ScienceLogic platform," notes Scott Martin, director of security compliance. "Prior to Black Duck, our process of managing open source was manual, yet as an organization we've always been committed to ensuring the security of our product. This presented a challenge which typically amounted to countless man-hours to ensure the security of our platform. Add in the fact that we've grown substantially over the past year, and we had the recipe for a painful operational challenge—ensuring the security and compliance of our code."

Why Black Duck?

"Both security and license compliance were equally important in our selection of Black Duck," says Martin. "I started investigating available tools, and the Black Duck solution was the most comprehensive. None of the other products could do a scan at as granular a level as Black Duck and also provide a comprehensive report that I can use to compile a list of open source software included in our product. Open source projects often have subprojects within them. Just because the main project is one license doesn't mean there's not something else within that project that will have its own licensing requirements or vulnerability issues."

> *"Both security and license compliance were equally important in our selection of Black Duck."*
>
> –Scott Martin, director of security compliance for ScienceLogic

Gaining visibility into what open source is actually in your codebase is the first step in securing your open source. Updated regularly from the National Vulnerability Database (NVD) and VulnDB, the Black Duck solution maps companies' open source libraries to critical metadata on vulnerabilities, licensing, community activity, and versions.

"Having access to additional vulnerability information via VulnDB is very important to us," notes Martin. "I need to be able to look at the vulnerabilities of all the different software packages we use and keep on top of any new vulnerabilities as they're discovered."

Through its KnowledgeBase™, Black Duck can show you which open source libraries are in use, as well as where and how they are used, and map known vulnerabilities in open source in use.

Black Duck continuously monitors your projects for newly identified vulnerabilities to give you the visibility and control to secure your open source software. It enables you to review and prioritize vulnerabilities, assign remediation dates, track closure, and manage security vulnerabilities before they become problems.

The results: Unmatched insight into open source code

"From a developer perspective, Black Duck gives our developers the ability to anticipate whether I'm going to say yes or no to a new piece of open source software they want to add," Martin says. "From a cost-benefit standpoint, I think of our use of Black Duck as an opportunity cost. How much time would it take and how many dollars would it cost to ensure there are no license compliance or security issues in the ScienceLogic platform if we weren't monitoring open source with Black Duck?

"The single biggest benefit to ScienceLogic is the visibility into the code that would otherwise take an immense number of man-hours," he adds. "What Black Duck does is put a light on open source code problems prior to release of a new version of our product. It's helped us correct issues, plus ensure we don't have similar issues in the future. That's really the value Black Duck has brought to us."

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

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

SYNOPSYS®
Silicon to Software™

01/16/19.cs-sciencelogic.