UROS
Exposing licensing and dependency conflicts in real time

Company overview

Since 2011, the Finnish multinational technology company UROS has led with imaginative engineering and a passion for challenging the status quo. UROS specializes in IoT, offering consumer and IoT connectivity solutions, along with cloud-based service platforms and connected hardware.

Its industry-leading solutions are grounded in a determination to make complex technologies simple for customers.

The government of India selected UROS as the technology provider for its National Jal Jeevan Mission. UROS Sense and UROS Flow solutions will help provide safe drinking water through individual tap connections by 2024 to all households in India.

To learn more about UROS, click here.

The challenge: Implement automated capabilities to expand visibility of licensing and vulnerability issues

The complexity and scale of today's development landscape demands a purposeful and holistic approach to AppSec practices and tooling. With ever-increasing development speeds, traditional security challenges are compounded by the shift toward DevOps practices. Security leaders are tasked with implementing solutions capable of adequately scaling and keeping pace with modern development cycles.

In the pursuit of a future DevOps model, UROS has undertaken an organizational shift toward automation and simplification. In the early phases of its software development life cycle (SDLC) transformation, UROS identified hidden licensing conflicts and obligations as a critical concern in its current model.

Jari Korkiakoski, chief security architect at UROS, noted that the lack of scope and scaling capabilities of its GitHub and open source scanners, along with the need to gain visibility into dependencies and corporate licensing obligations, were key challenges to its DevOps transformation. This challenge drove the company to look for an open source security solution capable of scaling to the growing business and providing automated insight into dependencies, license conflicts, and vulnerabilities.

The solution: Synopsys application security testing tools

UROS adopted Synopsys Black Duck® to help secure its open source and provide key insight into licensing conflicts and dependencies. The reasons for this choice included:

- Black Duck is a comprehensive software composition analysis (SCA) solution for managing the security, license compliance, and code quality risks that come from the use of open source in applications and containers.
  - **Dependencies.** Black Duck's integrations with most build tools allow UROS to track both declared and transitive open source dependencies in applications.
  - **Licensing.** Tracking and managing open source with Black Duck helped UROS avoid license violations that can result in costly litigation or compromise valuable intellectual property.

In the beginning phase of its AppSec transformation, UROS used Black Duck to help automate scan results and easily identify dependency and licensing issues in real time. When asked why UROS chose Black Duck, Korkiakoski stated, "Customers are starting to become more educated on security and they become increasingly involved in the security process, asking questions and demanding more visibility. With Black Duck's brand level of trust and proven track record, we are able to meet our customers' demand, address their concerns, and gain a competitive advantage."

> "Black Duck has helped us understand our overall security status, and find and fill security holes."
>
> —Jari Korkiakoski, Chief Architect

The results: Improved visibility, increased automation

Prior to implementing Black Duck, the company's open source was managed manually, with GitHub and custom-built open source scanners. This was not only labor-intensive, but it failed to identify hidden security concerns. UROS also couldn't scale this approach across its growing business and suspected that there were a multitude of unidentified concerns that needed to be addressed.

Korkiakoski noted numerous benefits that UROS now enjoys from the implementation of Black Duck—some of which were unexpected. While Korkiakoski was not surprised that Black Duck provided "great license coverage and improved visibility on hidden issues," he said his team didn't anticipate the overall improvement to its security practices. "[Our] security and services are becoming better—we have improved our security stance," he said.

UROS was surprised by the implicit dependencies in the software found in the first tests. The team was able to immediately identify both licensing concerns and dependencies quickly and with little effort, helping to jumpstart the security initiative.

Fundamental to the company's DevOps journey is the introduction of automation, wherever possible, into its pipeline. With Black Duck, Korkiakoski stated that security is now "…an ongoing process. Rather than ad hoc, security is automated, giving us a full understanding of our software stack." Crucial to this automation are Black Duck's real-time results. Korkiakoski noted that they hadn't seen this capability in other solutions. "[Black Duck] offers updating of previous scans, while you get results, all in real time. Notifications of these results let you make the right decisions."

With the help of Black Duck, UROS has seen its security posture rapidly improving, and now matching the reliability and reputation of its product offerings, solidifying its track record as a proven and trusted software provider.

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.

For more information about the Synopsys Software Integrity Group, visit us online at www.synopsys.com/software.

Synopsys, Inc.
690 E Middlefield Road
Mountain View, CA 94043 USA

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