MEGA INTERNATIONAL:
HOLISTIC APPLICATION SECURITY WITH COVERITY AND BLACK DUCK

Company overview

Founded in 1991, MEGA International is a global software company that has been a recognized market leader for more than 10 years. A leader in enterprise architecture, IT strategy, and business process analysis, the company partners with customers to leverage technology to improve governance and accelerate transformation. MEGA helps companies better analyze how they operate and make the right decisions to accelerate the creation of value.

"Coverity gave us a code quality approach that was very efficient, especially given the multimillion lines of code that needed to be scanned."

THE CHALLENGE: EXAMINING THE QUALITY, SECURITY, AND COMPLIANCE OF 5 MILLION+ LINES OF CODE

MEGA's flagship SaaS solution, the HOPEX Platform, enables organizations to plan and build upon their efforts around IT inventory, technical obsolescence, and IT strategy to manage governance, risk, and compliance; business processes; and data governance. "Our customers are major players, mainly in the financial and services industry, as well as government entities," said Philippe Bobo, MEGA's head of research and development. "All expect best-in-class security expertise and practices from MEGA, and secured code in our products and solutions."

MEGA's goal in working with Black Duck® was to validate that the more than 5 million lines of code in its software were as free from flaws as possible despite decades of enhancements and refactoring. "Another priority was to assure secure management of the ever-growing number of external libraries incorporated in our code," added Bobo. "This includes not only the libraries that we ourselves use, but also the libraries that they themselves may call. The dynamic hierarchy of dependencies can quickly become untraceable without a comprehensive and continually updated Software Bill of Materials [SBOM]. Lastly, we wanted to demonstrate to our SOC 2 auditors that our SaaS solution is securely managing data to protect the interests and privacy of our clients."

THE SOLUTION: HOLISTIC APPLICATION SECURITY WITH COVERITY AND BLACK DUCK

"Black Duck is a well-known leader in security, with an understanding of what is crucial to our global market, especially as it comes to the highly regulated financial services industry," said Bobo. "Partnering with Black Duck increases the credibility of our own security commitment."

"Black Duck demonstrated a thorough understanding of our business, and particularly of the challenges [and] the large number of software assets, legacy code, and compatibility issues that a long-time quadrant leader like MEGA has to deal with. This understanding made the implementation of Coverity® very straightforward."

"Coverity had the widest coverage in terms of coding languages," Bobo continued, "as well as a sharp approach to C/C++, with a highly satisfactory exception mechanism that would let us build a progressive picture of our code right from scratch, without being snowed under with a ton of alerts. This proved a key factor, as reliability was our main goal here."

"Black Duck SCA is the spearhead of our Bill of Materials initiative."

"We also had a need to understand and manage the third-party components and libraries we were using in our code, especially when it came to open source, and to build a thorough Bill of Materials detailing those components."

"Black Duck® SCA [software composition analysis] is the spearhead of our BOM initiative. Black Duck allowed us to quickly launch the exploration process and help us set alert priorities for a codebase that was becoming more and more complex. Time-to-value and completeness were our main goals here. Black Duck provided a very efficient and reactive consultant to help get us launched and to answer questions, and we became autonomous very quickly," said Bobo.

THE RESULTS: 40K DEFECTS FIXED, MORE THAN 1,700 OPEN SOURCE COMPONENTS IDENTIFIED

"As we anticipated, the Coverity and Black Duck scans caught dozens of forgotten or overlooked weaknesses in our software. Specifically, Coverity uncovered weaknesses that could affect the stability of the software, and in some cases, cast a light on the root causes of long-time unexplained occasional outages. Our teams have fixed close to 40,000 defect instances detected by Coverity since we began working with Black Duck in 2017."

"Using Black Duck almost immediately improved the level of control over our code by alerting our team to the security and license issues of some open source components," Bobo said. "Although we knew we were using open source libraries, we were still surprised by the number of libraries that were ending up in our package. In fact, Black Duck identified over 1,700 external components, and 70 different license types."

"Coverity and Black Duck allowed us to insert security and license compliance into the continuous integration process. Now, security and license noncompliance [issues] are raised to developers at the same time as functional or technical nonconformities, as a main contribution to our shift-left effort."

"The tools have also helped improve the housekeeping of the code," Bobo said. "Rather than fixing defects in legacy code that is not being used any longer, developers pare down their code. And rather than including new open source that requires legal approval of yet another license agreement, developers try to make more efficient use of already existing dependencies in their third-party components. When such approval is needed, the legal team directly connects to Black Duck."

"We would recommend Black Duck as a provider of a comprehensive set of holistic, complementary AppSec solutions, backed by a pool of sharp consultants who understand globally the industries they work with, as well as an organization's unique processes. For a B2B global organization like MEGA, it's a must," Bobo said.

About Black Duck

Black Duck® meets the board-level risks of modern software with True Scale Application Security, ensuring uncompromised trust in software for the regulated, AI-powered world. Only Black Duck solutions free organizations from tradeoffs between speed, accuracy, and compliance at scale while eliminating security, regulatory, and licensing risks. Whether in the cloud or on premises, Black Duck is the only choice for securing mission-critical software everywhere code happens. With Black Duck, security leaders can make smarter decisions and unleash business innovation with confidence. Learn more at www.blackduck.com.