

IGT Bets on Coverity to Secure Gaming Machines



“We have always had a 24/7 fault tolerant environment. With increasingly complex code, Coverity helps us maintain the exceptional level of code quality and security we’re known for in the industry.”

Steven LeMay
Director of Game Engineering, IGT



The IGT Challenge

IGT provides video and slot games for many applications, including traditional casino environments, Native American gaming, riverboats, and lottery environments. IGT has developed this diversity of product and expertise during 20+ years in the industry.

As the foremost supplier of these machines and systems world wide, IGT technology must pass through several rounds of review and approval. The first round of analysis is done statically, several times a week, utilizing Coverity Prevent. Then it goes to an internal product assurance team, and after passing the approval of this group, the software is sent to regulatory bodies such as the Nevada Gaming Control Board or test labs such as Gaming Laboratories International (GLI). At this critical juncture in the approval process, regulatory bodies have the authority to deny approval of the machine, which can delay a product’s time to market by as much as 6 weeks or even longer. The final approval ultimately belongs with IGT customers, who rely on the company to provide highly secure and reliable products.

Beyond the rigorous review process, IGT products are required to operate in a 24/7 fault tolerant environment. This means zero downtime and zero security vulnerabilities. It is a service level agreement of the highest quality, and the company’s internal motto for engineering.

With more than 1.9 million lines of code, IGTs code base has naturally grown in complexity over time due to the need to deliver increasingly advanced features. As overall complexity increased, IGT developers sought innovative technologies that could help them meet the demands of review processes and the company’s commitment to quality more quickly. Due to the size and complexity of this sophisticated code base, peer review and QA testing were becoming too time consuming based on the market appetite for new IGT products. To speed development while maintaining the company’s reputation for delivering high integrity code, IGT investigated static analysis as a solution that could complement the company’s existing manual code review and QA processes by automating the time intensive task of identifying security and quality defects in the source code.

Industry: Gaming

Business Challenge: IGT (International Game Technology) is one of the foremost suppliers of gaming machines and gaming monitoring systems in the world. The company recently introduced over 86 new games in addition to a complete new series of machine models. This release represented the single largest introduction of new products in IGT’s history. With customer expectations for 24/7 fault tolerance, a code base growing in size and complexity and an unmatched reputation for quality, IGT wanted a static code analysis solution that could bulletproof the security of their business-critical code early in the development lifecycle, when potential defects were easier and more cost effective to eliminate.

Results: IGT has all Coverity Prevent checkers turned on, automated Prevent scans and an ongoing established plan to be “Coverity clean”. In the software development environment IGT has created, no new Prevent defects are introduced to the main code base. The company is also using Coverity Prevent to ensure the quality of third party code, to completely insulate their code environment.

Solution

IGT chose Coverity Prevent due to its low false positive rate, which the company estimates to be less than 5%, and the high-value defects Prevent uncovered during a product trial. To ensure code integrity throughout the development process, IGT made Prevent part of the company's continuous integration process, where it runs automatically as a component of IGT's central build system. Developers at IGT also make use of Prevent's incremental analysis on an ad hoc basis to test code on their desktop, prior to submitting it to the central build system.

After every completed Prevent scan, automatic email notifications with specific defect results are sent to the developers responsible for introducing a given defect. From a management perspective, IGT has a specific number of defects they require to be corrected every week. With objective, automated information available about the continuing improvement of their code, data from Prevent helps IGT development leaders ensure no new defects are created as their applications progress toward release.

In addition to eliminating potential quality defects, IGT developers take painstaking care to eliminate any potential security vulnerabilities from their code. The software development organization takes every measure to ensure that the code is secure, including the review and elimination of even parse warning errors. In some industries, parse warning errors are commonly regarded as benign defects, but in the high stakes environment that IGT competes in, they can be a sign of more serious issues in the code. According to Steven LeMay, Director of Game Engineering at IGT, "Even parse warning errors can help identify other hard to detect problems. Because of its accuracy, we feel every possible issue reported by Coverity Prevent is worth further investigation."

In addition to reviewing internally developed code, IGT also uses Coverity Prevent to analyze 3rd party code to intercept any potential new defects that could be introduced by externally developed code. The use of third party code is unique in the gaming industry because producers of gaming software are only allowed to use certain code components from external vendors such as drivers and operating systems – all actual game code is written by licensed IGT engineers. LeMay continues, "In addition to helping IGT find bugs as early as possible, another benefit of Coverity Prevent is that it provides a single source of information regarding potential defects the code we create as well as the 3rd party code we receive."

Details

Security checkers in Coverity Prevent help developers improve their code by detecting malicious inputs and insecure coding practices. Because user applications have become increasingly prone to malicious input from end users, it's critical for IGT to understand

and track user generated data and how it propagates throughout an application. Without a full picture of the software system, malicious inputs could be overlooked. Specifically, IGT has found that the `STRING_OVERFLOW` checker can identify when malicious inputs are being copied to other strings. In addition, the `TOCTOU` checker shows the developer that filenames may be unsafely checked before they are being used, creating a possible file-based race condition.

"We turn on all the security checkers in Prevent. We don't care about the severity of the defect, we fix them all. We won't tolerate any possible security threat, and if Prevent indicates one may be present – that's enough to merit further investigation," said Steven LeMay. Additionally, there are standards regarding functions in code that IGT applies which are designed to prevent security defects from happening. LeMay continued, "Prevent automatically flags suspicious functions in our code, allowing developers to specify internal functions that they want to deprecate."

For IGT, another important Coverity Prevent feature is trend analysis, which the company uses for management reporting as well as empirical evidence that can be reviewed by government regulators as proof that IGT code is secure. Trend analysis also gives IGT's lead developers visibility into the number of new defects being introduced over time, allowing them to track the overall progress of their software releases from a quality and security perspective. These metrics provide value to engineering managers as they establish quality objectives and to build confidence in the code being produced.

"With a false positive rate under 5%, Coverity Prevent began finding potentially critical defects for us immediately. It required only a few days to integrate, a few months to achieve widespread developer adoption, and it's now a critical step in our coding process."

Steven LeMay
Director of Game Engineering, IGT

Conclusion

Across IGT's large and talented staff of developers, Prevent has proven its ability to identify hard-to-find defects for even the most experienced developers. With a constantly growing team, Prevent is of extra assistance to newer developers at IGT. LeMay notes, "Prevent saves our most experienced developers much of the time that used to be consumed by manual review of code from junior developers. Prevent is also a great tool to help educate junior engineers about proven programming practices." This frees LeMay's most senior development leads to focus on higher level design and code reviews because they entrust early defect detection to Prevent.

IGT developers have saved significant time by relying on Coverity Prevent to automate defect detection. This has allowed developers to focus on checking in cleaner code to the central build system, avoid the introduction of new security or quality defects, and helps ensure IGT's continued success with its rigorous regulatory approval process. A summary of results includes:

- With a false positive rate under 5%, Coverity Prevent enjoyed early and widespread adoption due to its highly accurate results.
- Objective, automated information from Prevent about potential security and quality defects assists IGT through the rigorous stages of regulatory review with auditors from organizations such as the Nevada Gaming Control Board or test labs such as Gaming Laboratories International.
- When receiving 3rd party code, Prevent provides an early and objective means to assess the integrity of outsourced code and avoid the introduction of new defects.

About IGT

International Game Technology (<http://www.IGT.com>) is a global company specializing in the design, development, manufacturing, distribution and sales of computerized gaming machines and systems products.

Free Trial

Request a free Coverity trial and see first hand how to rapidly detect and remediate serious defects and vulnerabilities. No changes to your code are necessary. There are no limitations on code size, and you will receive a complimentary report detailing actionable analysis results. Register for the on-site evaluation at www.coverity.com or call us at (800) 873-8193.

About Coverity

Coverity (www.coverity.com), the software integrity company, is the trusted standard for companies that have a zero tolerance policy for software failures, problems, and security breaches. Coverity's award winning portfolio of software integrity products helps customers prevent software problems throughout the application lifecycle. Over 100,000 developers and 500 companies including ARM, Phillips, RIM, Rockwell Collins, Samsung and UBS rely on Coverity to help them ensure the delivery of superior software. Coverity is a privately held company headquartered in San Francisco with offices in 6 countries and more than 150 employees.

Coverity Inc. Headquarters

185 Berry Street, Suite 1600
San Francisco, CA 94107 USA
U.S. Sales: (800) 873-8193
International Sales: +1 (415) 321-5237
sales@coverity.com
www.coverity.com
scan.coverity.com

Coverity Asia Pacific

Shinjuku Nomura Building 32F
1-26-2 Nishi-Shinjuku, Shinjuku-ku,
Tokyo 163-0532, Japan
Asia Pacific Region Managing Director
Rich Cerruto
Phone: +81-3-5322-2978
japan_sales@coverity.com
coverity.com/index_jp.html

Coverity EMEA

Farley Hall, London Road
Binfield, Bracknell
Berkshire, RG42 4EU
England
emea_support@coverity.com