MEND | IGT

Mend Prioritize
IGT's Game Changer

Automatically find and fix open source vulnerabilities
using Mend's free tools in your own environment

About IGT

IGT is the global leader in gaming. It is listed on the New York Stock Exchange under the trading symbol "IGT," and its holding company headquarters are in the United Kingdom, with operating headquarters in Rome, Italy, Las Vegas, Nevada, and Providence, Rhode Island.

The Company attracts the industry's top talent, with more than 12,000 employees across the globe.

The Challenge

When it comes to keeping its applications secure from known vulnerabilities, global gaming giant IGT is at the top of its game.

With offices in Beijing, Belgrade, Warsaw, London, Providence, Reno, Las Vegas, and San Francisco (just to name a few), IGT's team of over 2,000 developers are working around the clock to produce applications for lotteries, land-based and digital gaming, and more.

The company does business with gaming and lottery operators in more than 100 countries around the world. With its scale, IGT's applications face a diverse and stringent set of regulations, international standards, legislation, and certifications that it must meet when it comes to the security of its products. IGT complies with the rules and guidelines for handling payments and privacy set by ISO, the E.U. General Data Protection Regulations (GDPR), World Lottery Association (WLA), U.S. Multi-State Lottery Association (MUSL), and Payment Card Industry (PCI), as well as local requirements of more than 300 gaming commissions and boards.

While responsibly offering entertaining content for their customers' players, they must consistently meet the highest levels of data security and safety. Due to the sensitive security concerns for the data being processed and stored by their applications, IGT takes application security exceedingly seriously, employing a sizable security team and adopting the most advanced AppSec technologies to secure their applications throughout the Software Development Lifecycle (SDLC).

> *Our reputation and the confidence of our clients is based on IGT's ongoing vigilance and the continuous security of our systems and applications. We simply cannot tolerate a breach.*

Open source security has been one key area of focus for IGT's development team in recent years as they rely more on open source components to keep up with their fast-paced deployment schedule.

Along with their implementation of a Mend to detect and remediate open source components with known issues early in the development process, IGT has been one of the early adopters of Effective Usage Analysis technology that gives them a significant advantage in their remediations.

This technology has been shown in Mend's research to dramatically reduce the scope of relevant alerts by over 70%.

The Mend Solution

For IGT's security and development teams, managing the influx of incoming vulnerability alerts for their massive stable of applications can feel like bailing out a sinking ship with a fork.

Pleskonjic says that IGT's developers have faced fatigue from high rates of false positives produced by other AppSec tools noting that "they spend a lot of time analyzing and there is no real effect."

When it came to open source security, they faced the challenge that even though they trusted the information from the alerts, they lacked an objective way of prioritizing which vulnerabilities were the most pressing for remediations.

Mend's Effective Usage Analysis technology has been a game-changer for Pleskonjic and his team, providing them with a simple way to cut over 70% of their security alerts and focus on the most urgent vulnerabilities that demand their attention. Effective Usage Analysis assesses the security impact of each open source vulnerability based on whether it is being used in the product or not, depending on if the proprietary code is making calls to the vulnerable functionality.

"There are times when we receive alerts about seemingly important libraries, but then Effective Usage Analysis will show us that our application isn't actually using the vulnerable method," explains Pleskonjic on how they are able to reduce the number of alerts requiring their attention. "By filtering out these alerts, we are able to focus our efforts on fixing the vulnerabilities that really matter and achieve better security levels and lower security risks. It's something that is really, really helpful to us."

Pleskonjic estimates that Effective Usage Analysis has helped bring down the time spent on remediations by nearly half.

"Effective Usage Analysis decreases the amount of work for our developers," explains IGT's Senior Information Security Engineer Vladimir Jelic. He cites how developers can understand at a glance from the Mend dashboard which vulnerable open source components are effective depending on the color of the shield next to it. "If they see the green shield, then they immediately know that they can move on to a more pressing alert."

The Results

Beyond the time savings, Pleskonjic and Jelic say that Effective Usage Analysis has gained developer trust by presenting them with vulnerabilities that are relevant and trustworthy, making it a tool that they want to use.

"Our team was already happy with how Mend has helped us to manage our open source security," says Jelic on the positive feedback from their developers, adding that, "Now with these new features from EUA, we can continue to spread that positive impression throughout the development teams."

About Mend

Mend, formerly known as WhiteSource, effortlessly secures what developers create. Mend uniquely removes the burden of application security, allowing development teams to deliver quality, secure code, faster. With a proven track record of successfully meeting complex and large-scale application security needs, the world's most demanding software developers rely on Mend. The company has more than 1,000 customers, including 25 percent of the Fortune 100, and manages Renovate, the open- source automated dependency update project.

Related Resources

For more information, visit www.mend.io, the Mend blog, and Mend on LinkedIn and Twitter.