Digital.ai App Security
for gaming

Add security directly into your gaming apps

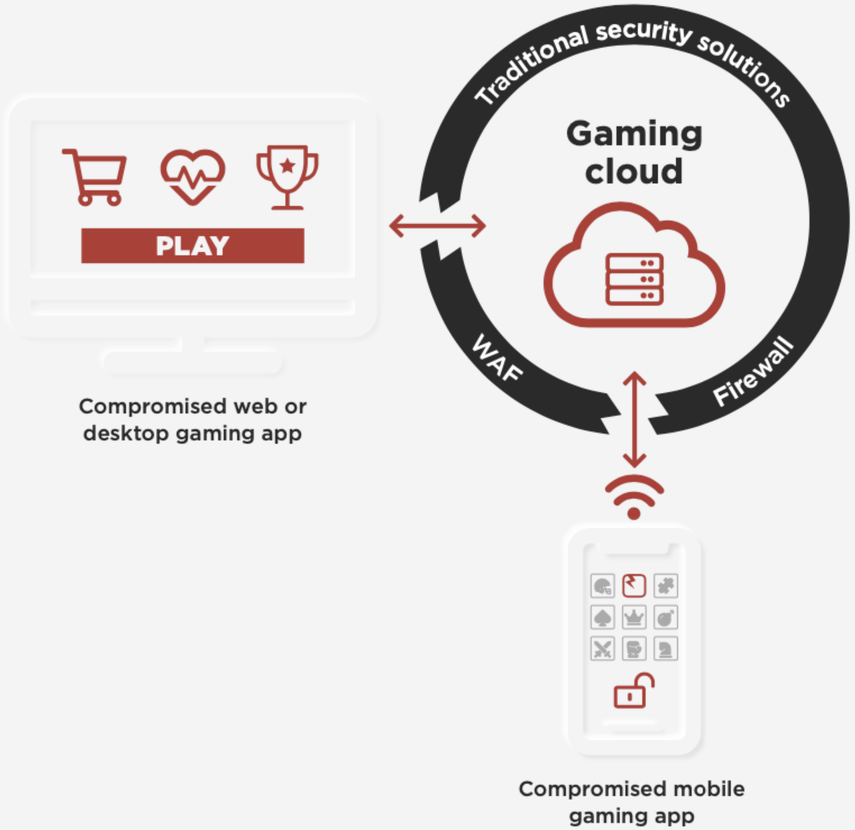
More than 3 billion people play console, mobile, and online video games. According to Newzoo's latest Global Games market report, players will spend about $176 billion in 2021, with more than half of that money coming from the mobile segment.

Gaming apps represent a unique attack vector to bad actors. Video games are now the world's largest entertainment industry, with consumers shifting preferences from legacy television to mobile phone devices for media viewing. The average time spent on a mobile device has outgrown set-top boxes by eight minutes daily on average.

The gaming industry incorporates user and financial data systems uncommon to other businesses. Personal account information, in-game transactions, and buyer-seller marketplaces utilizing credit cards are common elements of a gaming app ecosystem.

Players trust that gaming companies are protecting their personal information through a robust security practice. Unfortunately, under-resourced companies are forced to favor production release deadlines over security. As a result, gaming apps are viewed as high-value targets by bad actors.

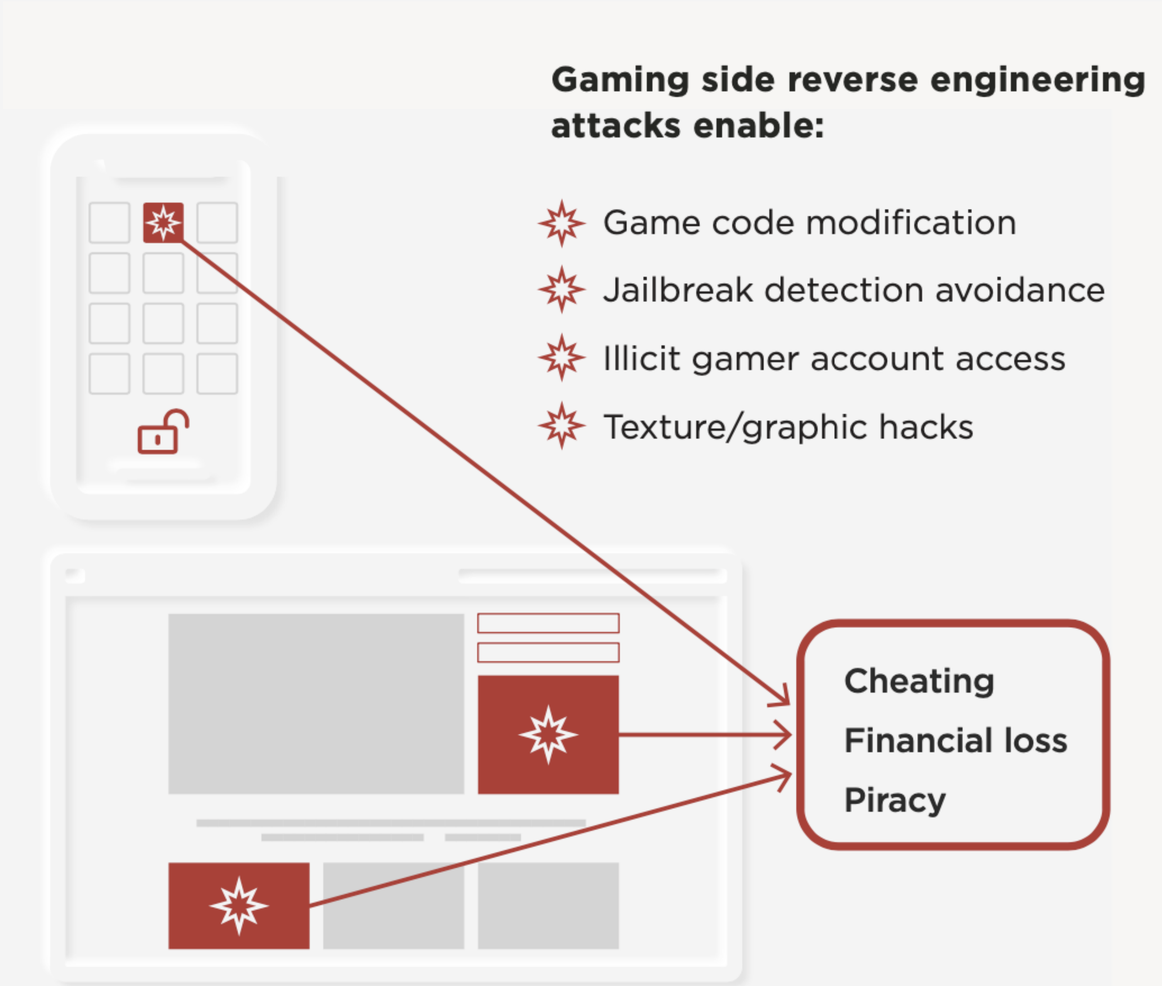
The impact of a successful attack can be financially catastrophic to game publishers. A compromised game reduces the chance of mega-success and can even result in the cancellation of a game altogether. Avoiding these scenarios by implementing mobile app security practices is paramount for the long-term success of all gaming apps and gaming studios.



Game source code: Playground for bad actors

Using commonly available tools, bad actors can manipulate mobile and PC game code with relative ease, therefore providing a clear path to develop cheats, break digital rights management software, and insert malware.

For gaming studios maintaining a considerable portfolio of apps, the risk of attack increases. A typical DevOps schedule amounts to a constant cadence of code updates, fixes, and releases. Faced with the result of an impossible task of security code maintenance, the probability of protecting a staggering collection of apps is lowered significantly, therefore underscoring the requirement for an app security solution

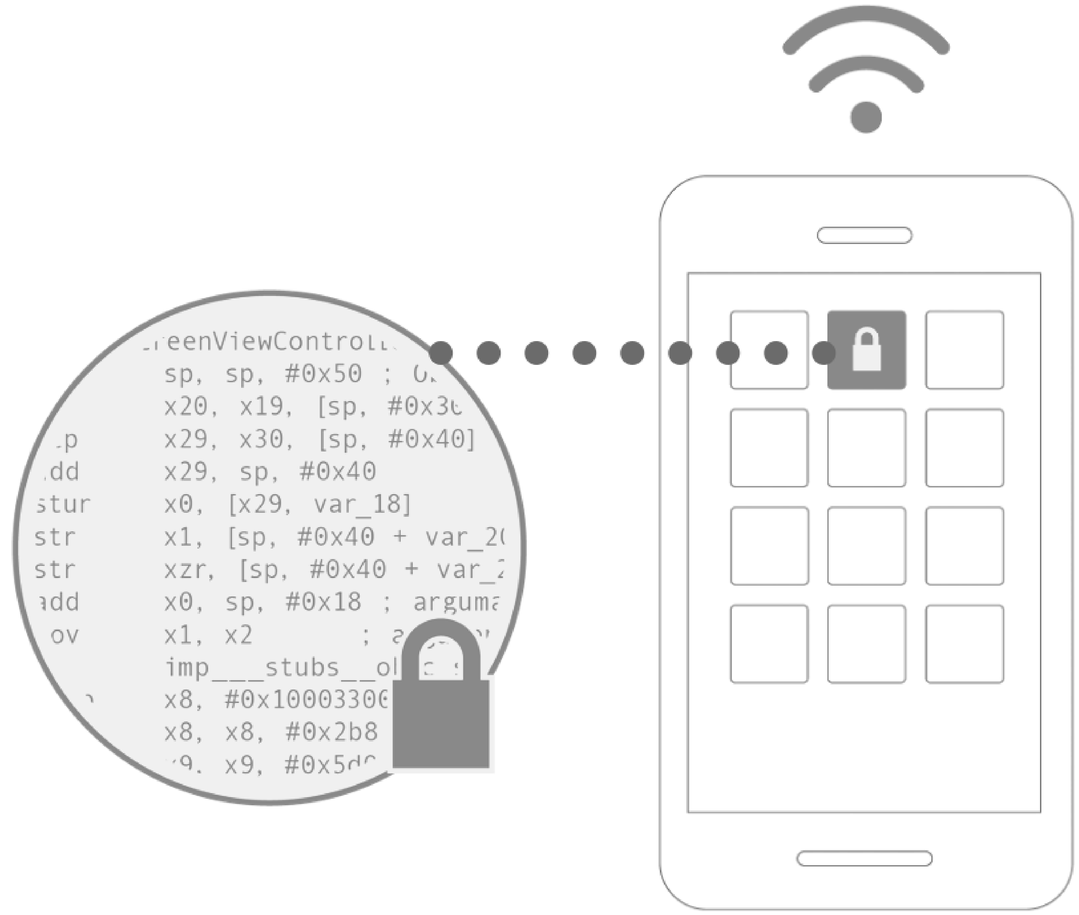


Turning gaming app security inside out

Digital.ai Application Protection, formerly Arxan, stops attacks where they happen because it is integrated at the binary and source code level. This multi-layered approach can be applied to subsequent code revisions automatically, which greatly reduces the effort required when updating apps for release.

Furthermore, protecting games with Digital.ai Application Protection helps secure mobile, PC, and web app games without disrupting the game development lifecycle:

• Obfuscation of code — Hiding code makes it difficult for attackers to reverse engineer an app. Through code obfuscation, viewing and reverse engineering is time consuming for attackers. Hiding code doesn't eliminate these actions altogether and should be used in conjunction with additional app security methods.
• Self-defense and integrity preservation — Automated app defense prevents bad actors from cloning gaming apps, developing cheats, and injecting malicious code.
• Detection and the feedback loop — Real-time threat data serves as an early warning of attacks in progress. Threat data is utilized in development feedback loops to improve and implement app protections.



Digital.ai App Protection, formerly Arxan, obfuscates source code, detects when apps are running in unsafe environments and reports on threats to the applications you create and deliver.

Closing the loop with Digital.ai App Aware

Detection and response are key to deterring app attacks, while maintaining a proactive state of readiness against bad actors. When data is collected and utilized within the software development feedback loop, decisions and updates are implemented with agility.

Digital.ai App Aware significantly advances the speed and accuracy of closing the feedback loop. Game publishers are better equipped with visibility into app attacks. As a result, publishers form decisions that preserve the state of business.

The feedback problem

The absence of threat data, which outlines a gaming app's security posture after release, removes the ability of developers to rapidly respond to attacks.

Threat data feedback into the development process is commonly left unaddressed by commercial game protection solutions. Either the gaming publisher is required to create a feedback loop, or be faced with having zero real-time threat data collected, monitored, and analyzed from a collection of released games.

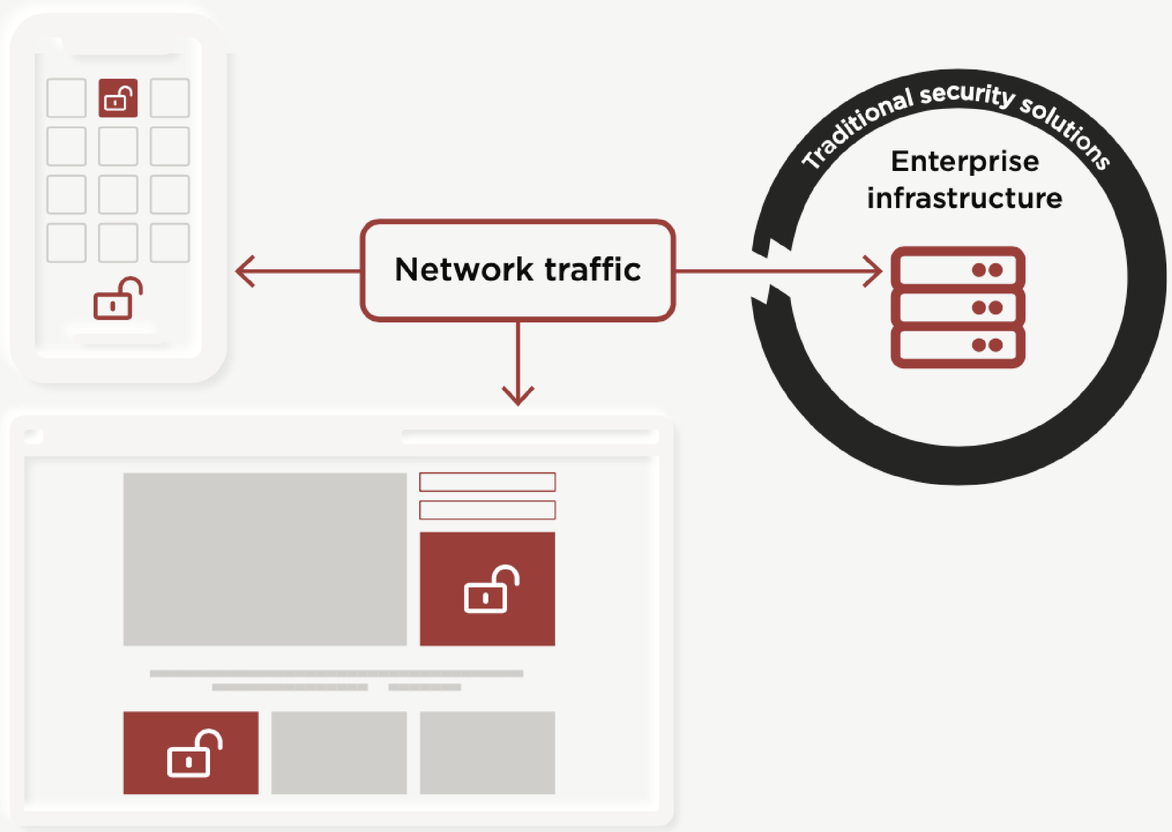
Without active threat understanding, the probability of exploitation of mobile gaming apps is heightened. Gaming studios able to gather attack data and close the feedback loop will be empowered to make informed security decisions. Correlated feedback allows developers to observe, decide, and adapt apps to counter attackers in real-time. As a result, interested parties can be agile in crafting responses and preserve the core business.

Actions taken may include shutting down compromised account access, creating separate in-game instances to which cheaters can be automatically banished, forever banning cheaters to stir discord within online communities, and dynamically updating game protections to counter zero-day security vulnerabilities — all achievable when based on analytics data.

Extend protections

As a benefit for the continuity of an entire gaming operation, Digital.ai solutions also protect and maintain game network traffic integrity through:

- **Key and data encryption to secure critical information and downloadable content (white-box cryptography)**
- **Web code protection to protect “in the clear” JavaScript (obfuscation)**



Meeting the needs of gaming publishers

Digital.ai protection solutions enable gaming publishers to protect gaming apps by adding protection from bad actors seeking to exploit vulnerabilities and violate the integrity of encryption keys — while also adding the features of real-time threat intelligence.

Digital.ai's unique approach of securing code after the development cycle adds to the efficiency of the DevOps lifecycle — ultimately addressing the challenge of securing gaming apps.

Digital.ai protection solutions allow gaming publishers to extend the life of gaming apps by preventing reverse engineering, eliminating financial fraud, and maintaining business continuity and company brand.

To learn more about how Digital.ai can protect your gaming applications, schedule time to speak with one of our product experts.

Digital.ai/contact

About Digital.ai

Digital.ai is an industry-leading technology company dedicated to helping Global 5000 enterprises achieve digital transformation goals. Using value stream management as its cornerstone, Digital.ai combines innovative technologies in agile planning, application protection, software delivery, and artificial intelligence into a unified Value Stream Platform. Digital.ai makes it possible to connect software development and delivery efforts to strategic business outcomes and create secure digital experiences customers trust.

Learn more at Digital.ai