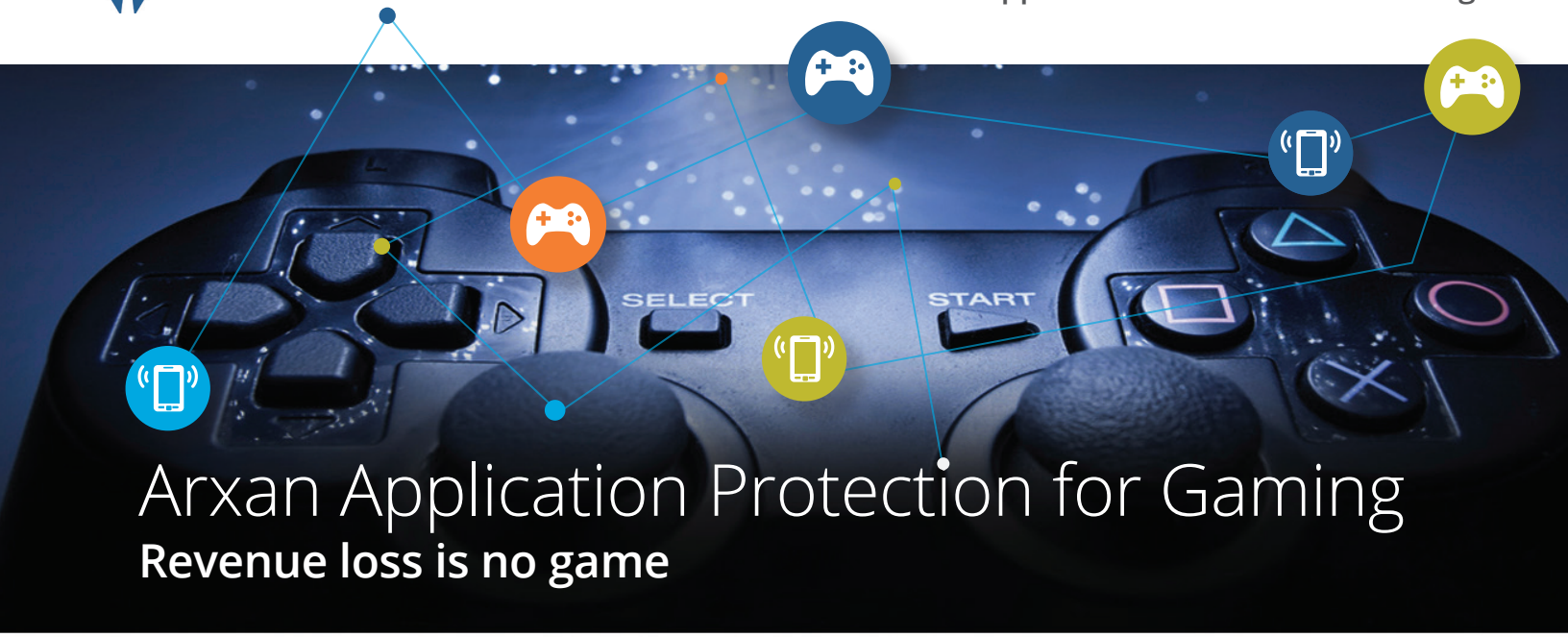

Arxan Application Protection for Gaming

Revenue loss is no game

Relentless: Your Game and Reputation are on the Line

Gaming has become a battle between studios and hackers. Whether it's a MMOG (massively multiplayer online game), console or a graphically-rich PC game, gaming software is extremely vulnerable to attacks on the client and/or server. Hackers reverse-engineer game protocols to steal intellectual property (IP) or inject malware, modify code to enable piracy or cheating, and even clone back-end servers for independent game operation. These attacks can result in substantial revenue loss to illicit client usage or cloning of client or server applications to affect game play. The resulting monetary and business risk to game publishers, studios and distributors is significant.

Top Gaming Attacks You Must Defend

Hackers continue to unleash relentless attacks on games by:

- **Tampering to cheat.** Cheating is the biggest threat to the popularity and value of a game. Hackers tamper client functionality to unfairly benefit the hacker.

- **Tampering for piracy** Piracy is the biggest threat to game profitability. Since hacks are often released within hours of new game titles, versions, or other virtual world assets, they decimate new revenue. Hackers enable piracy by tampering with a PC game to de-activate, spoof or bypass license management.

- **Reverse-engineering the client app.** For PC games and the client portions of on-line and mobile games, hackers can have complete control of game execution at run- or rest-time, to unravel internal logic and client-server communication. They can then exploit vulnerable code with cheats, clone clients or issue commands.

- **Reverse-engineering to clone the back-end server.** Attackers can model a back-end server by analyzing client communications with the server and internal client operations. This then enables a "clone" of the back-end server to be created and run independently of the game operator, thereby stealing subscription revenues.

- **Reverse engineering communication.** As the client and server, or two peers, communicate in the virtual world, hackers can inspect data traffic to reverse-engineer protocols. Subsequently, simple tools can be used to block packets and produce a negative effect on a player, or to replay packets that produce benefits for the hacker.

Arxan Protects Your Game and Keeps Revenue Flowing

Arxan is the trusted leader in gaming attack-prevention and self-protection. Arxan's solution proactively defends against tampering and reverse-engineering to protect security logic, including DRM routines. Arxan also uses a variety of techniques, including obfuscation, so client code remains confidential and unauthorized changes to program functionality are prevented. Since hackers also love to clone popular games then collect subscription revenues from their cracked copies, Arxan protects the integrity of the game's brand, assets, stories and characters. Features include:

- Code protection against reverse engineering
- Fortification of game logic from tampering
- Key protection to secure client/server communications and game assets

Why Choose Arxan? Your Reputation is Everything.

Gaming customers appreciate the technical and business value our application protection delivers.

- **Security Strength:** multi-layer guard network delivers the most advanced application protection
- **Maturity:** we are protecting apps running on more than 500 million devices
- **Simplicity and Customizability:** integration is easy and security protection maps to your specific requirements
- **Service and Support:** world-class support from experts who are available when you need them
- **Trust and Stability:** financially strong company backed by top tier private equity firm; customers represent some of the world's leading brands

Arxan Automated Application Protection

DEFEND

Against reverse engineering, tampering and any manner of theft

DETECT

An attempted attack on the application code, or on another Guard

DETER

Attacks by safely exiting or silently deleting illegal assets or stealthily reporting back forensics information to a command center