# Use Case: Online Video Gaming

Compared to movies, television, and music, online gaming is the largest entertainment industry today. Combined, social, mobile, free-to-play and pay-to-play massively on-line multiplayer gaming is projected to grow to nearly $200 billion by 2022. Players often trust a great deal of their personal information to gaming companies just as they would with their employer, online retailer, and banking institutions. Much of this personal information includes financial details from in-game purchases and monthly subscriptions. This hoard of data has caught the attention of hackers. In the last 2 years, the top 9 gaming data breaches resulted in the loss of approximately 73 million players' personal and financial information.

The suspected underlying reasons the gaming industry is the subject of so many breaches begin with video game companies being pushed to use low-friction authentication measures to avoid customer attrition and revenue loss; as with most businesses, time is money and fast paced game release cycles introduce security risks; and finally, the singular focus on games – data security is now an equal priority. Gaming companies have determined that misconfigured servers and insider leaks have enabled the most recent gaming data breaches.
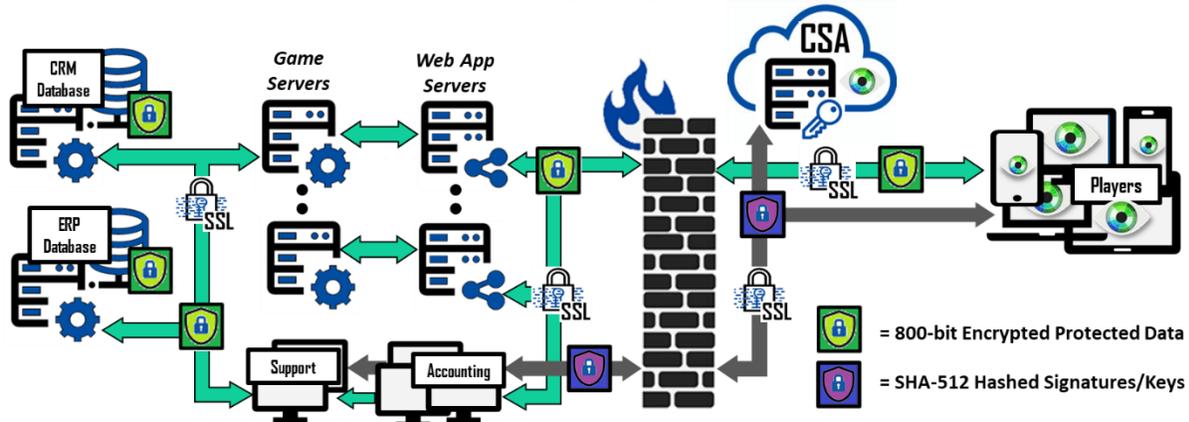
Bonafeyed's Data Defined Security protects critical data whether in the player CRM databases, the transaction ERP databases or on a gamer's tablet, PC, or smartphone. A player's ID (login), password, PII data, and payment information is encrypted by Cy4Secure before it leaves the player's device and remains encrypted throughout the gaming eco-system, including game servers and databases. Encrypted in-game purchases and billing information can be viewable by the accounting and billing departments. Support and Accounting could access encrypted CRM data. However, not all encrypted fields need to be accessible by all departments or employees. For example, marketing and sales can create reports on demographics, consumption, and revenues, but they do not need to decrypt a majority of the PII or payment information to obtain business analytics. Cy4Secure only allows authorized use of encrypted data.

The gaming world brings joy, fun, and even a learning experience for many players. Protecting personal information has now become as important for game developers as it is for the banking, healthcare, and retail industries. To prevent exploitation and monetization of players' breached data, developers can use CY4Secure to encrypt data at the source, and keep it encrypted until it is accessed or read by an authorized user. The most cybercriminals can obtain is unintelligible/encrypted data that has no value on the dark web. Contact us at info@bonafeyed.com for a demonstration or visit us at www.bonafeyed.com.