sonraí SECURITY

INDUSTRY REPORT

Gaming Industry Guide To Identity and Data Security Across the Public Cloud

Whether you're an indie developer, work for a AAA publisher, or somewhere in between, you'll want to secure your data and identities in AWS, Azure, and GCP.

Online games have been popular since the 1970s. In recent years, they have increased to include single and multiplayer games played on mobile devices and tablets the public cloud. However, as the online gaming industry continues to grow, the number and severity of security risks are becoming a serious challenge for most gaming organizations.

The gaming industry is big business. So much so that Statista predicts that the global video game market will be worth a staggering $138 billion by the end of 2021, and estimates that there are currently almost 2.5 billion video gamers worldwide.

The rising demand for improved quality applications, products, experiences, services, and information has driven the culture shift in the gaming industry. One of the most significant ways organizations are adapting to rising demand is by shifting security left in development cycles. For example, by migrating regulated workloads to platforms such as Google Cloud Platform (GCP), Amazon Web Services (AWS), and Microsoft Azure, organizations can efficiently address speed innovation issues, competitive pressures, and time to market.

Organizations are approaching the security of the public cloud cautiously. The importance of security in gaming is an essential consideration for all companies that handle consumer and financial data.

Despite the potential risks posed by cloud technology, it still offers incredible opportunities. The challenge for organizations like yours is to innovate in the cloud without creating risk for stakeholders and customers. This balance is achievable through various steps; Defining your cloud governance standards, creating real-time automation that enforces governance, risk management, compliance policies, identity security, and continuous monitoring.

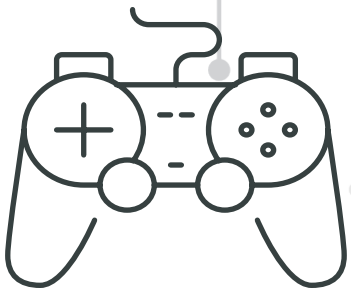
This guide explores how your gaming organization can approach innovation with a roadmap for reducing risk, increasing security, enforcing compliance and improving operational efficiency in the cloud.

Lots of Games = Lots of Players

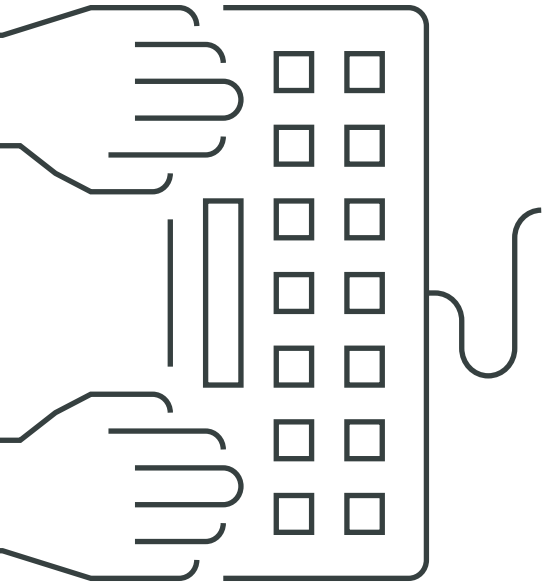
Video games have evolved over the last several decades into a thriving entertainment business. With Internet availability becoming widespread, one of the factors in the growth of games has been online play. Which includes session-based multiplayer matches, massively multiplayer virtual worlds, and intertwined single-player experiences.

While single-player games remain popular, multiplayer games have captured the attention of gamers who want to play against each other online. Massively Multiplayer Online (MMO) games are now the most popular type of game for online players. This genre includes roleplaying, strategy, and first-person shooting games. Despite criticism, online games — especially

MMOs — have become a multi-billion dollar industry. Each major MMO is, essentially, a business enterprise in itself. The success of these games depends on satisfactory experiences from multiple stakeholders, including game creators, investors and, of course, players. Keeping players entertained and securing their identities and data presents a challenge to gaming organizations.



sonraí SECURITY



Popularity Brings Increased Risks

Online games have always drawn a crowd. The cloud has enabled this explosion by centralizing gaming data and opening its opportunity to an ever-widening global community. Technology facilitates simultaneous game streaming across various devices, numerous platforms, and multiple formats. Every player can access something that interest them.

Cloud services meet the ever-increasing demands of players, and build a great player experience that have become a crucial aspect of a game's success. For developers, a simple infrastructure that provides timely insights is the key to getting the game right while also providing an exceptional player experience.

However, there are more opportunities for data leaks, data access, and mistakes when developing games in the cloud. The growing number of gamers encourages providers to deploy complex architectures across the public cloud and satisfy high demand. For example, MMOs rely extensively on sophisticated applications, built on massive distributed architectures to deal with the real-time interaction of thousands of concurrent users. Any breaches at any point in the gaming delivery channel can cause sufficient damages and loss to shut down any game permanently.

Many Games, Many Risks

The speed of game development opens the industry to misconfigurations, policy violations, threats, and identity and data security challenges.

Bad Actors & Insider Malice

The simplest and one of the more common risks is when an employee, or a person identity, uses legitimate permissions for malicious activities. People may take a position within a company to gain access to sensitive data, and formerly trustworthy employees might expose valuable information.

In April 2020, an ex-Naughty Dog employee leaked key moments from the video game company's yet-to-be-released second game, including major spoilers, that ruined the anticipation of the games release for many people. It is predicted that this employee did this due to unfair treatment by the Naughty Dog staff. Thousands of fans were heartbroken as the much-anticipated game was completely spoiled.

Someone with sufficient privileges and a reasonably good understanding of security may be able to set-up one or more overprivileged "sleeper" identities, allowing them to do an extraordinary amount of damage.

According to Happy Power, a popular Fortnite fan on YouTube, someone who works for Epic Games has been the source of many leaks about the company's releases. It's possible the unidentified person uses a sleeper identity.

Misconfigurations

Human mistakes will happen and will not be deliberate at times, but these errors can still wreak havoc in an organization. Despite the massive amounts of intellectual property, PII, and crown-jewel data stored by game developers, the gaming industry is relatively new to cybersecurity when compared to other industries like finance and healthcare. Game development and publishing studios often face the nightmarish task of protecting huge amounts of revenue and data with modest security. There is a tendency to greatly prioritize ease of use in the user experience over security. This security gap can lead to human error and misconfigurations.

In August of 2020, Razer accidentally leaked personal information for over 100,000 gamers after a researcher discovered that the customer data on the technology company's website was publicly available on August 18th because of a server misconfiguration.

De-risk Your Cloud By Securing and Locking Down Your Data

As you shift to cloud operations and quickly develop games, a primary concern is compliance and the security of your data and business architecture. Your developers are responsible for creating fast, secure, and flexible applications that offer financial services to your clients without any risk of data exposure. Don't take these risks lightly. The financial industry is a favorite for hackers for obvious reasons. Also, it is one of the most regulated industries due to the sensitivity of data it deals with and the critical nature of its systems.

Some of the regulations that protect consumers include: The Gramm-Leach-Bliley Acts, Sarbanes-Oxley, Payment Card Industry Data Security Standard (PCI DSS), and the most recent General Data Protection Regulation (GDPR). Contrary to popular belief, the challenges associated with information security are not specific to the IT department. The legal and reputational ramifications from a data breach could adversely affect the entire organization, especially when an organization loses the trust of its clients or attracts severe fines for data governance non-compliance.

Sonrai Dig provides your organization with the agility of the cloud without compromising security or compliance. It de-risks your cloud by finding possible holes, helps you fix them, and prevents these problems before they occur. Sonrai Dig works by monitoring your resources, data, and microservices, monitoring your database services to get real-time feedback on the health state of your public cloud, looking for object stores and public buckets, and monitoring access to these resources. While working with Sonrai Dig to de-risk your cloud, the goals are to:

- Eliminates identity risks in your cloud by getting and maintaining least privilege
- Locks down your most important data to avoid mistaken data exposure
- Integrates your security, audit, DevOps teams, and IAM to shift left effectively
- Fixes occurring problems and prevent them from occurring in the first place

Get To and Maintain the Principle of Least Privilege

Regulation of the principle of least privilege involves determining what is sufficient permissions. Sonrai Dig uses advanced analytics to monitor the various identities and data relationships closely. It ensures that identities only receive minimum permissions to meet their goals and avoids any risk of excessive privilege. Detailed graphs allow you to visualize all the identity to data relationships, making for easier management of the organization. Effective regulation of least privilege helps reduce errors such as privilege escalations, toxic combinations, and separation of duties. The principle of least privilege works to ensure there are no security threats from within the company either by accident or on purpose.

Shift Left to Integrate Teams

Sonrai Dig provides collaborative arrangements early enough in the data management process, which helps companies develop efficient systems from the very beginning. A useful tool is the swimlanes, which organize the clouds by access rights and teams. Swimlanes ensure that the right information reaches the right units for prompt responses and timely remediation.

Remediation and Prevention of Issues

Sonrai Dig offers a well-structured platform that works to prevent data issues and achieve a high-performance structure for your organization's public cloud. The platform escalates identified issues to the right bot or team immediately.

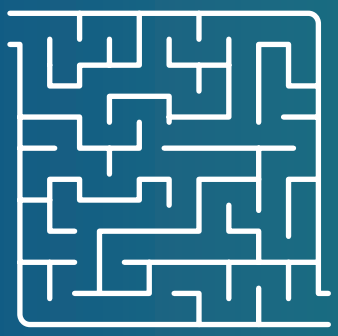
Locking Down Crown Jewel Data

The goal of Sonrai Dig is to reduce the blast radius of any potential security concern. It does this by finding solutions, classifying them, and de-risking your organization's crown jewel data. The crown jewel data is locked down with an impenetrable system that comes with an inbuilt alarm system that sends out a signal in case of any unexpected or sudden activity.

Today's online gaming industry provides an excellent example of why organizations require enhanced cloud security.

Firstly, gamers often use their personal information to purchase and play games, including banking data, addresses, phone numbers, etc. Sometimes, popular MMOs have millions of players, each of whom has individual information that they have trusted to the provider. The exposure of any single element of one person's PII could result in significant losses to the gamer for which the provider may be liable.

Secondly, online gaming security has traditionally focused on preventing piracy and intellectual property theft. The creatives were more concerned about someone stealing their idea/graphics/plots/ etc. than they were about keeping their game player's information safe. Hacks, PII thefts, and expensive downtimes have informed game providers that upping their security game is integral to their business success as is their gaming strategy.



Finally, too, that cyber thieves who find a vulnerability in one file or game will use the same sleuthing strategies to see it in other files or games. And since games themselves aren't governed by sophisticated data security regulations, any single gaming vulnerability is likely to be found in more than one game.
The result? Many disappointed gamers and one dead gaming company.

Sonrai Dig Helps Gaming Orgs

The Sonrai Dig platform is unique. It streamlines and manages 'identity' as the critical key to data access and ensures all users are subject to the 'Principle of Least Privilege.' This principle guarantees that users only access the data they need at that moment for a particular purpose.

For gaming companies, this identity and access management (IAM) strategy covers all entities accessing every game, from individual human users to 'roles,' instances, serverless functions, and containers, any of which contributes to any element of the game. The platform provides equally sound IAM oversight regardless of whether the game is played in AWS, Azure, GCP, or Kubernetes environments.

Game providers must comply with the GDPR if it collects any personal data from EU citizens or residents. The Sonrai Dig platform facilitates the internal auditing of this personal data to ensure it's managed according to the regulation. The platform also alerts providers when it discovers security risks that could affect gamers' personal information and generates reports that provide evidence of compliance.

How Sonrai Dig Works

Sonrai Dig monitors every identity (person, or machine) and every resource (database, compute programming, etc.) across a multi-cloud platform with multiple third-parties, cloud accounts, vendors and other entities. Dig analyzes all possible relationships and graphs those interactions to inform the automated alerts that sound when the system detects an inappropriate connection.

The platform's simplicity facilitates the agility needed for gaming by relieving provider IT professionals to focus on those intricacies, not on maintaining security standards. Using Dig to watch over cloud-occurring interactions allows innovation to occur safely and securely.

Benefits of Using Sonrai Dig

Increase Security

Sonrai Dig's continuous access monitoring prevents security breaches. Its data and identity-centric security approach finds, classifies, minimizes access, and continuously monitors all Crown Jewel data in structured and unstructured stores.

Reduce Risk

Sonrai Dig eliminates risk, other solutions cannot see. Patented graph analytics, superior integrations, and intelligent collection find identity, data, and network risks impossible to see without Sonrai Dig. Automation eliminates the risk.

Maximize Efficiency

Sonrai Dig increases innovation velocity while reducing costs. Swimlanes, role-based access, DevOps workflows, and automation ensures security while increasing DevOps team agility. Customizable objectives simplify playbooks while solution breadth eliminates redundant tooling.

Enforce Compliance

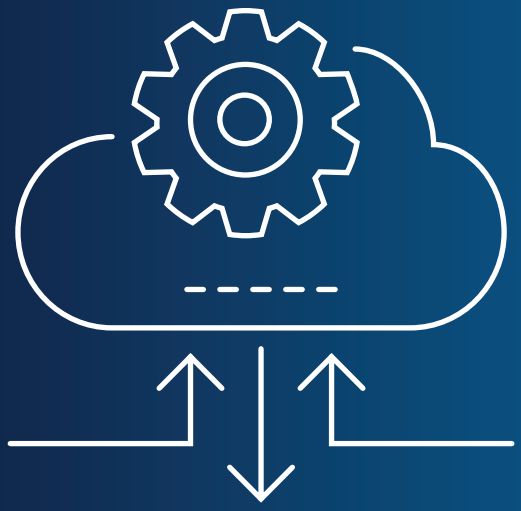
Sonrai Dig is the most complete compliance platform. With over 1000 control policies and 30 frameworks spanning data, identity, cloud-platform and container compliance mandates Sonrai Dig is the most comprehensive cloud and security continuous compliance platform.

sonraí SECURITY

Benefits of using Sonrai Dig

Manage CSPM

Sonrai Dig allows you to effectively utilize the speed and agility of cloud technology to monitor the cloud and container infrastructure. At the same time, the platform enforces the strength of your cloud posture and cloud security. The automation of remediation and detection of cloud misconfigurations gives you insight into errors that could violate policy or breach security. It also helps increase profitability, productivity, and innovation while significantly reducing risk.



Continuously Audit

Sonrai recognizes that to maintain efficiency, companies should regularly conduct internal audits because they help identify possible non-compliance issues before external auditors. However, lack of time and sufficient resources are constant reasons given to excuse lacking to perform internal audits. Sonrai helps remedy this making the audit process less time-consuming. Additionally, through automation Sonrai provides reports and evidence of compliance, significantly cutting down the auditor's hours and consequently saving money for your organization.

Delivery of Complete Risk Models

When dealing with data in the cloud, it is essential to monitor and identify all the ways it has been and can be accessed to deploy security measures such as data and identity governance properly. Sonrai Dig eliminates risk, other solutions cannot see. Patented graph analytics, superior integrations, and intelligent collection find identity, data, and network risks impossible to see without Sonrai Dig. Automation eliminates the risk.

See Our Platform in Action

Contact us today to get your free demo and be that much closer to achieving best-in-class cloud security.

Sonrai offers a demo for gaming organizations to correctly identify holes such as; escalations, separation of duty, excessive privilege, and possible risks across the roles and compute instances within your cloud. Our demo helps show you how to identify what has access to your data, what is accessing your data, what could access your data, and what changes have occurred.

Learn More

Sonrai Security offers a demo for gaming organizations and brings you that much closer to data security and compliance. See how we identify holes such as excessive privilege, escalations, separation of duty, and potential risks that may arise from the identities, permissions, and data exchange within and across clouds.

Request a demo today!

sonraísecurity.com
info@sonraísecurity.com
646.389.2262