imprivata

INFOBRIEF

How digital identity management strengthens the security posture of gaming organizations without compromising workflow efficiency

There's a saying in the gaming world: the house always wins.

But what happens when the house comes up against a player with an incalculable edge, not bound by any rules or code of ethics?

How can casinos and other gaming establishments level the playing field?

Cybersecurity threats are a major risk to the gaming industry. One research study found that online gaming is the industry third most likely to experience a cyber attack. Another study found that 51% of organizations – in every industry – have experienced a data breach from a third party.

From ransomware to malicious insiders to payment card fraud, there are no shortage of sophisticated cyber threats emerging.

Hackers and other bad actors see casinos and other gaming establishments for what they are – lucrative financial targets processing a massive volume of payment card transactions in possession of their guests' personal data.

That's why the winning play for anyone operating in the gaming industry is simple: turn to a digital identity management solution that optimizes security and creates a streamlined workflow for casino staff.

Challenges impacting the security of organizations in the gaming industry

When a malicious actor unleashes a cyberattack on a casino, the potential impacts include operational disruption, financial losses for the casino and guests, the theft of guests' personal information, and a loss of reputation for the gaming establishment.

To avoid these impacts, the answer is to implement proper cybersecurity controls that safeguard guests as well as the business as a whole. But doing that isn't easy. Here are just a few examples of the obstacles that need to be overcome:

- **Maintaining regulatory compliance |** State gaming commissions have a multitude of regulations related to security or access management for staff, privileged users, or vendors.
- **Increasing cyber insurance |** As cyber threats grow in size, scope, and magnitude, insurance providers are asking policyholders to adhere to much more stringent security controls.

- **Unique user workflows |** Many casino floor operators such as pit bosses, slot techs, front desk workers, and floor staff use the same workstations. This leads to challenges around identity management which act as a major security vulnerability. On top of this, an inability to use mobile devices on the casino floor prompts a need for alternative methods of multifactor authentication.
- **Complex technology environments |** Many casinos have a mixture of cloud and on-prem applications which may have varying user authentication requirements. They also likely have a variety of vendors and third parties requiring access to their system.

Strategic solutions

Protecting staff and guests while staying compliant with state regulations is no easy task. Having a well-defined, comprehensive digital identity management strategy can play a key role in enhancing an organization's overall security posture and introducing a more efficient workflow for its staff.

Knowing what to do and how to do it can seem overwhelming, but here are the main tenets a solid security strategy should include:

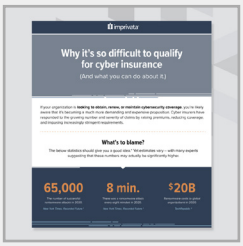
- **Meet cyber insurance requirements to secure and maintain coverage |** To maintain coverage, cyber insurance providers want casinos and other gaming organizations to have capabilities such as multifactor authentication, privileged access management, and complex user passwords, among others
- **Mitigate the risk of cyberattacks |** Gaming organizations may not be able to prevent a potential attack from occurring with 100% certainty, but there are actions they can proactively take to minimize the damage they might face
- **Improve workflow efficiency |** Staying secure shouldn't come at the expense of sacrificing operational efficiency, so frictionless access to applications is crucial
- **Simplify user access – but keep a detailed audit trail |** Streamline and monitor user activity across shared endpoints in the case cages, hotel front desk, and other locations
- **Secure third-party access |** Maintain secure and transparent access for all Class II and III vendors
- **Streamline compliance |** Ensure compliance with PCI as well as state and federal requirements

Want to learn more? Check out these resources to better understand how Imprivata can help gaming establishments optimize both security and efficiency:

Datasheet - The Third-Party Remote Access Solution for PCI DSS Compliance

Whitepaper – The proven ROI of SSO

Video - Seamless access into cloud and on-premises applications with Imprivata



Infographic – Why it's so difficult to qualify for cyber insurance

To enact the best digital identity management strategy, organizations should partner with a trusted provider of digital identity solutions. Imprivata is that industry-leading partner.

The Imprivata difference

Driven by extensive experience and expertise, Imprivata is uniquely positioned to help organizations in the gaming industry overcome security, workflow efficiency, and regulatory compliance challenges. Benefits include:

- **Unmatched support delivering user-friendly workflows on shared endpoints,** greatly reducing risks surrounding generic user accounts without sacrificing efficiency for casino and hotel floor staff
- **Quick, flexible, user-friendly authentication** to satisfy multifactor authentication requirements, while providing users with options to best meet their workflow needs (including options that are not phone-based, which complies with polices forbidding the use of mobile devices in the cash cage or elsewhere on the floor)
- **Single sign-on for both legacy and cloud applications,** resulting in a fast, secure, consistent authentication experience for both IT and floor staff
- **Faster time to value** through lightweight, cost-effective, and easy-to-implement solutions for privileged access management and vendor access management
- **Standardized processes for secure third-party and vendor access management,** creating a cost-effective path for casinos who want to manage all their vendors in the same secure, automated fashion

Partnering with Imprivata, a casino can keep its staff focused less on technology and more on delivering a high-quality, signature experience for guests.

They can free up more time for strategic projects and initiatives after improving IT operational efficiency.

And they can more dependably meet regulatory requirements and reduce cybersecurity risks with more robust security controls.

Request demo

imprivata®

Imprivata is the digital identity company for mission- and life-critical industries, redefining how organizations solve complex workflow, security, and compliance challenges with solutions that protect critical data and applications without workflow disruption. Its platform of interoperable identity, authentication, and access management solutions enables organizations in over 45 countries to fully manage and secure all enterprise and third-party digital identities by establishing trust between people, technology, and information.

For more information, please contact us at:

Global headquarters USA
Waltham, MA
Phone: +1 877 663 7446
www.imprivata.com

European headquarters
Uxbridge, England
Phone: +44 (0)208 744 6500
www.imprivata.com/uk

Germany
Langenfeld
Phone: +49 (0) 2173 99 385 0
www.imprivata.com/de

Australia
Melbourne
Phone: +61 3 8844 5533

1286-2023_infobrief-gaming-industry