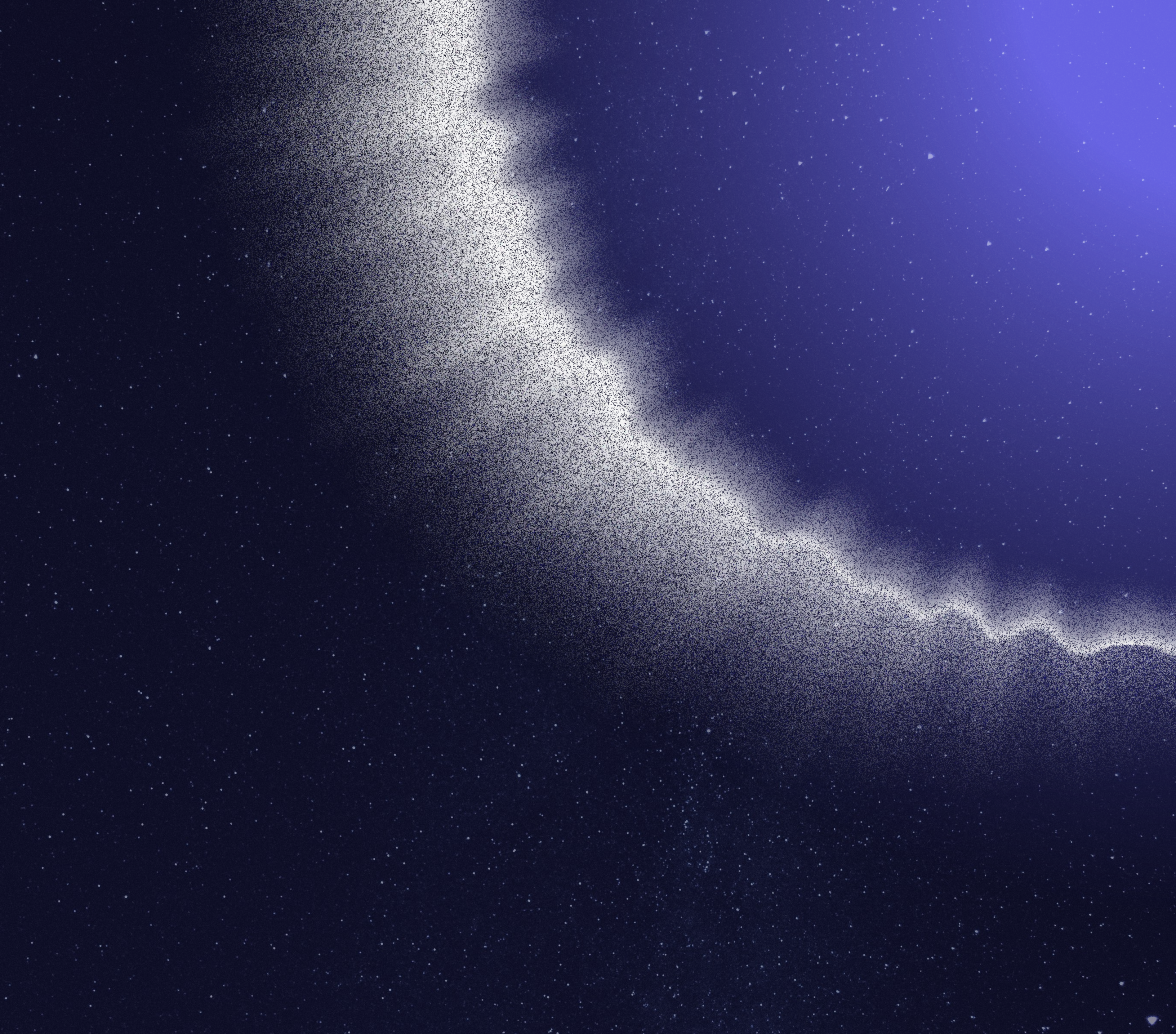
High Stakes Cybersecurity

UPPING THE ANTE FOR INTELLIGENCE POWERED CYBERSECURITY

CENTRIPETAL



Casinos are a magnet for millions of players each year, generating billions in transactions across physical venues and online platforms.

The casino gaming industry injects nearly $329 billion into the U.S. economy annually, as reported by the American Gaming Association.

With 1.6 million regular gamblers and 4 million annual participants, the stakes are high. By 2025, the global online gambling market is expected to skyrocket to $113 billion.

Current Trends in Casino Cybersecurity

In July 2023, the FBI highlighted several evolving trends in the ransomware landscape, directly impacting casinos. Ransomware actors are exploiting vulnerabilities in vendor-controlled remote access to casino servers and utilizing legitimate system management tools to elevate network permissions.

Between 2022 and 2023, ransomware attacks on casinos via third-party gaming vendors surged, primarily targeting smaller and tribal casinos. These attacks often result in encrypted servers and compromised personal information of employees and patrons.

The Casino Industry Cyber Threat Landscape

As the digital landscape continues to evolve, casinos must fortify their defenses to safeguard their operations and customer data against this growing menace. **These alarming trends underscore the high-risk nature of the casino industry.**

Phishing Attacks

A staggering 80% of cyber incidents in the casino industry stem from phishing attacks.

Rising Incidents

Cybersecurity incidents in the casino sector have surged by 40% over the past three years.

High-Risk Sector

Casinos rank as the third most targeted sector for cyberattacks

Challenges Facing the Casino Sector

The gaming industry is often built on outdated technology, making both games and entire casino floors susceptible to cyberattacks. Regular patching, updates, and improvements are crucial. Neglecting these can lead to severe consequences, such as system-wide shutdowns due to malware or ransomware.

From Q4 2021 to Q1 2022 alone online attacks on the global gaming community increased by

260%

Cybercriminals exploit both technical and resource vulnerabilities through various tactics, including DDoS attacks, ransomware, theft, fraud, phishing, and human errors.

Casinos are subject to some unique challenges that drive decisions about cybersecurity:

Financial Fraud

Casinos are prone to financial fraud, including counterfeit currency, credit card fraud, and money laundering. Robust anti-fraud measures like transaction monitoring systems and Know Your Customer (KYC) procedures are essential to prevent and detect fraudulent activities.

Emerging Technologies

The adoption of AI, IoT, and blockchain brings new security challenges. Staying current with technological advancements and implementing proactive security measures is vital to mitigate these risks.

Cyberskills Retention and Burnout

In the casino industry, retaining cybersecurity skills is critical due to the sector's reliance on digital infrastructure and the constant threat of cyberattacks. However, the high-stress environment and the continuous need for vigilance contribute to burnout among cybersecurity professionals, making retention a significant challenge.

High-Profile Cyber Incidents

In September 2023, MGM Resorts, one of the world's largest casino operators, suffered a cyberattack disrupting operations across multiple Las Vegas Strip properties. Slot machines, ATMs, digital key cards, electronic payment systems, and online reservations were affected, resulting in an estimated $100 million loss and significant operational challenges. Both MGM Resorts and Caesars faced ransomware demands, with one company complying with the hackers' extortion requests while the other resisted, underscoring the ransomware threat in the gaming industry. Additionally, Marina Bay Sands in Singapore reported a breach exposing personal data of about 665,000 non-casino rewards program members.

In response to escalating cyber threats such as the Nevada Gaming Commission (NGC), have introduced new cybersecurity regulations for gaming operators. These regulations mandate securing systems, conducting risk assessments, monitoring cybersecurity risks, and timely disclosing cyberattacks

Three Strategic Steps to Maximize the Potential of Intelligence Powered Cybersecurity for the Global Online Gaming Sector

01 Utilize the Latest Threat Intelligence for Real-Time Protection

Leverage the latest threat intelligence from the cybersecurity community and industry to enhance your defensive posture. Blocking malicious and reconnaissance traffic before it enters the network eliminates threats before they can cause harm, enhancing the protection of sensitive customer data and the integrity of gaming operations.

02 Collaborate with Cybersecurity Experts Using AI and Human Intelligence

The scale of cyber protection is now so vast that leveraging industry-wide expertise is essential. Partnering with cybersecurity experts who utilize powerful AI-enabled tools and deep industry knowledge can significantly bolster your defenses against a wide array of threats. Casinos and online gaming platforms can benefit immensely from these collaborations, enhancing their security measures without overextending their resources.

03 Join a Cybersecurity Data Sharing Community

Security incidents in one gaming platform or casino can often occur in others as well. By sharing threat data, organizations can collectively improve their defenses. Geographic and sector-specific communities can exchange experiences, indicators of compromise (IOCs), techniques, and resolutions. Sharing threat data is increasingly becoming a regulatory requirement. Immediate strategic gains can be achieved by working with experts who can interpret and rapidly deploy community learnings, strengthening the overall cybersecurity posture of gaming companies. The recent mandates from the Nevada Gaming Commission are indicative of this evolving obligation.

THE SOLUTION: PROACTIVE PROTECTION WITH CLEANINTERNET®

> “This morning I had zero events. I refreshed three times just to make sure. Sure enough we had no events thanks to Centripetal."
>
> Incident Response Analyst, Information Technology at a Pacific Gaming Casino

Centripetal's CleanINTERNET® solution presents a tailored approach to the unique needs of casinos and global online gaming platforms. In an environment where customer data and gaming integrity are under continuous attack, CleanINTERNET® harnesses real-time threat intelligence from a global network, providing visibility into potential threats before they can affect your systems. This technology serves as a protective barrier, ensuring the security of sensitive information.

CleanINTERNET® is an intelligence powered security solution that utilizes high-performance computing technology, patented software algorithms, and highly skilled security analysts to offer a cost-effective alternative protection strategy. Casinos and online gaming platforms that have adopted CleanINTERNET® are impressed by its comprehensive capabilities, which far exceed basic intelligence feeds. Achieving a similar security posture independently would be financially unfeasible.

CleanINTERNET® revolutionizes cybersecurity by prioritizing threat intelligence and shifting from reactive to proactive defense. This enhances the efficiency and effectiveness of security teams. With advanced shielding technology, CleanINTERNET® eliminates the majority of threats and mitigates the impact of any malicious code that breaches defenses. The technology blocks malicious network attempts from known sources, prevents outbound activity to malicious domains, and eliminates unnecessary reconnaissance traffic from your network.

By implementing CleanINTERNET®, casinos and online gaming platforms can quickly bolster their cyber defenses without significant financial investment or the need to expand their cyber analyst teams. This solution greatly reduces the number of security events, allowing IT teams to focus on maintaining operational efficiency with greater confidence.

IT’S TIME FOR THE CASINO INDUSTRY TO DOUBLE DOWN ON INTELLIGENCE POWERED CYBERSECURITY

Casinos, with their substantial financial assets, are prime targets for cybercriminals. The sector's reliance on outdated technology and the rapid adoption of emerging technologies further complicates the cybersecurity landscape. IT professionals in the casino industry must prioritize regular updates, robust anti-fraud measures, and compliance with regulatory standards to safeguard against the evolving threats.

For casinos and online gaming platforms, embracing intelligence powered cybersecurity solutions is not just an option; it’s a necessity. By being proactive, you can transform your defenses and ensure robust protection for your sensitive data and gaming operations. Take the lead in cybersecurity innovation and safeguard your operations against the threats of today and tomorrow.

As cyber threats evolve, vigilance is crucial. Casinos must understand both the expanding attack surface and the increasingly malicious tactics of cybercriminals. Strengthening cyber preparedness protects your organization’s future success.

Stay vigilant, stay updated, and ensure your defenses are as formidable as the games you host.

CENTRIPETAL

centripetal.ai