

**PLAYING BALL WITH
INTELLIGENCE POWERED
CYBERSECURITY**



CENTRIPETAL

The sports industry is a multifaceted powerhouse, seamlessly blending digital and physical worlds, protecting sensitive customer and player data, and often playing on a global stage.

This complexity demands that sports organizations stay vigilant against a myriad of security threats.

[According to the National Cyber Security Centre](#), a staggering 70% of sports organizations experience at least one cyber attack annually. With the global sports market projected to soar to [\\$623.6 billion by 2027](#), cybercriminals are quickly eyeing this lucrative sector.

The Digital Playbook

The digital revolution in sports has brought unmatched convenience and insights, but it has also unleashed a host of cyber vulnerabilities. From high-profile sporting events to major league associations, and from entertainment venues to online ticket sales, the landscape is a goldmine for cyber threats. Sports organizations house treasure troves of information—athletic performance data, competitive advantages, and sensitive consumer information—all of which are prime targets for cyber adversaries.

The interconnected nature of modern sports venues, brimming with networks and devices, presents new avenues for attacks. Malware deployment, data theft from point-of-sale systems, and phishing scams targeting online ticket sales have become commonplace. This labyrinth of threats necessitates a robust and united front from sports authorities, cybersecurity experts, and the global community.

Cyber Sidelined: Case Studies of Cybercrime in the Sports World

In November 2020, [Manchester United](#) faced a ransomware attack that crippled its digital operations. The club swiftly disconnected its systems to halt the ransomware's spread, collaborating with cybersecurity experts and law enforcement to investigate and contain the incident. Remarkably, they restored their systems without succumbing to the ransom demands.

Similarly

20,000

employees and fans had their sensitive information compromised when the [San Francisco 49ers fell victim to a ransomware attack](#) in 2022.

The organization compensated victims, stressing the impact of breaches. [In March 2023, the NBA reported a data breach at an external provider](#), exposing fan details and highlighting third-party vulnerabilities.

Triple Play: Turbocharging Cybersecurity in Global Sports

Beyond the allure of financial gain, other factors amplify the vulnerabilities within the sports sector. The intricate web of vendors collaborating with sports organizations creates numerous access points ripe for exploitation. Additionally, the limited technical teams on-site, preoccupied with streaming events or handling fan transactions, often overlook cybersecurity measures due to the complexity of managing vast systems.

Legacy systems, not designed with modern security practices in mind, and a lack of awareness about emerging cyber threats, further exacerbate these risks.

Athletes, affiliate sports organizations, and even fans must be educated on recognizing phishing emails and avoiding suspicious links. **Vigilance and preparedness are essential to thwart these threats.**

01

Strike First with Cutting-Edge Threat Intelligence

Stay ahead of the game by tapping into the latest threat intelligence from the global cybersecurity arena. Block malicious activity before it breaches your network, safeguarding your critical data and ensuring seamless operations. In the high-stakes world of sports, preemptive defense is your winning strategy.

02

Team Up with Cyber Experts for AI-Driven Defense

In the vast playing field of cyber protection, leveraging expert knowledge and AI technology is a game-changer. Collaborate with top-tier cybersecurity specialists who bring AI and human intelligence together. This partnership fortifies your defenses against a multitude of threats, allowing sports organizations to stay secure without stretching resources thin.

03

Join the Cybersecurity League for Data Sharing

In sports, teamwork is key, and the same goes for cybersecurity. By sharing threat data within your industry, you can collectively strengthen defenses. Sector-specific communities exchange vital information, such as indicators of compromise and effective countermeasures. This collaborative approach not only meets regulatory requirements but also rapidly enhances your cyber resilience.

The Game-Winning Solution: CleanINTERNET® for Proactive Protection

Centripetal's CleanINTERNET® delivers a custom-fit cybersecurity solution tailored for the dynamic needs of the sports industry. With real-time threat intelligence sourced globally, CleanINTERNET® offers a shield against potential threats before they disrupt your systems. This technology acts as a critical line of defense, protecting sensitive information with unmatched precision.



“With one security person here on staff, having almost a redundant SOC that comes in the form of the incident responders and forensics folks that Centripetal layers on top of its hardware solution that sits in front of my firewall is a really powerful combination.

I have a second set of active eyeballs that's looking at my environment, which deals with 200 million incidents per day.”

VP of Technology Operations and Information Security for The Boston Red Sox

CleanINTERNET® combines high-performance computing, patented algorithms, and skilled security analysts to deliver an economic and superior protection strategy. For sports organizations, this solution outperforms basic intelligence feeds, offering comprehensive security without the hefty costs associated with many security solutions.

By prioritizing threat intelligence and transitioning from reactive to proactive defense, CleanINTERNET® revolutionizes cybersecurity. This approach boosts the efficiency of security teams, blocking all known threats and minimizing the impact of any breaches. It prevents malicious network attempts, thwarts outbound connections to harmful domains, and eliminates unnecessary reconnaissance traffic.

Implementing CleanINTERNET® allows sports organizations to enhance their cyber defenses swiftly, without substantial financial investment or the need for larger analyst teams. This solution significantly reduces security incidents, enabling IT teams to focus on maintaining operational excellence.

THE URGENCY FOR CYBER DEFENSE FOR THE SPORTS INDUSTRY

In the fast-paced sports industry, adopting intelligence powered cybersecurity solutions is a necessity, not an option. By proactively transforming your defenses, you can ensure robust protection for your critical data and operations. Lead the charge in cybersecurity innovation and shield your organization from evolving threats. As cyber threats become more sophisticated, staying vigilant is essential.

Sports organizations need to consider the growing attack surface and the ever-evolving tactics of cybercriminals. Strengthening your cyber defenses today secures your organization's success in the future.



centripetal.ai