Mitigating AI-powered Deepfake Cybersecurity Attacks in Sport

TIAKI

Off-field deepfake threats are increasing for high profile sports franchises

In the fast-paced world of sports, high-profile franchises are not only competing on the field but also in the digital realm where cyber threats loom large. With the rise of AI-powered deepfake attacks posing a significant risk to the integrity and reputation of global sports organisations, the need for robust cybersecurity measures has never been more critical. This blog brief explores how Secure Access Service Edge (SASE) can play a pivotal role in addressing the cybersecurity risks associated with AI-augmented deepfake attacks on high-profile sports franchises.

The impact of deep fake cyber attacks on global sports leagues that have just signed billion dollar media rights deals can be profound. **Deepfake incidents increased 60% in 2024**, establishing **AI-powered deepfake attacks as the fastest-growing type of adversarial AI currently impacting the market**. Leading research forecasts that these **deepfake attacks could lead to over $40 billion in damages by 2027[1].**

The combination of the influx of private equity and substantial billion-dollar sports media rights deals raises concerns about leading sports leagues such as those in the NFL, MLB, NBA, NHL, Premier League, IPL, and Rugby Championship. These leagues and sports franchises may now be at greater risk and perceived as easy targets by AI-powered cyber criminals. Given this scenario, implementing Secure Access Service Edge (SASE) can play a crucial role in neutralising the threat posed by AI-powered deep fake attacks in the sports industry.

Understanding the deepfake threat in sports

AI-powered deepfake attacks have emerged as a potent weapon in the hands of cybercriminals, enabling them to create highly realistic and deceptive audio, video, or text content that can be used to spread misinformation, manipulate public opinion, or deceive individuals. For high-profile sports franchises that are benefiting from recent billion-dollar media rights deals, the potential impact of deepfake attacks on their reputation, financial stability, and fan base cannot be underestimated.

The proliferation of AI-generated voice and video fabrications is eroding trust in institutions and governments by blurring the boundaries of believability. Deepfake techniques have become so prevalent in nation-state cyber-warfare entities that they have evolved into a mature attack tactic among nations engaged in constant cyberwarfare interactions.

In the contemporary commercial landscape, AI advancements like Generative AI and deepfakes have transformed from simple misinformation tools into sophisticated instruments of deception. The increasing sophistication of AI has made it progressively difficult to differentiate between authentic and manipulated information.

In a recent C-suite survey, **62% of CEOs and senior business executives, anticipate that deepfakes will introduce operational costs and complexities for their organisations within the next three years, with 5% viewing it as an existential threat[2].**

---

[1] https://venturebeat.com/security/deepfakes-will-cost-40-billion-by-2027-as-adversarial-ai-gains-momentum/
[2] us-generative-ai-and-the-fight-for-trust.pdf

Gartner forecasts that by 2026, the utilisation of AI-generated deepfakes in face biometrics attacks will lead to 30% of enterprises no longer considering these identity verification and authentication solutions as reliable in isolation[3].

The increasing deepfake business risk

The risk to sporting franchises is increasing dramatically whilst the C-suite of sporting franchises may not be fully aware of the rapid progress in the threat and potential impact on their business models. The deepfake risks to sporting organisations include:

1. Reputational damage:
Deepfake attacks can manipulate videos and audio to create fake content that can damage the reputation of a sports franchise. This can lead to loss of trust from fans, sponsors, and other stakeholders.

2. Financial loss:
A deepfake attack can result in financial loss for a sports franchise through decreased ticket sales, sponsorship deals, and merchandise sales. It can also lead to legal costs associated with defending against false claims.

3. Data security breach:
AI-powered deepfake attacks can be used to steal sensitive data from a sports franchise, such as player contracts, financial information, and fan data. This can result in financial loss, legal consequences, and damage to the franchise's reputation.

4. Competitive disadvantage:
Deepfake attacks can be used to manipulate game footage or player interviews to give a rival team a competitive advantage. This can impact the performance of the team and result in losses in games and tournaments.

5. Regulatory compliance issues:
Deepfake attacks can violate regulations related to data privacy, intellectual property rights, and consumer protection. This can lead to legal consequences, fines, and damage to the franchise's reputation.

The role of SASE to address exposure to deepfake threats

Secure Access Service Edge (SASE) is a comprehensive cybersecurity framework that combines network security and access control capabilities into a single, cloud-native solution. By integrating networking and security functions into a unified platform, SASE offers high-profile sports franchises a holistic approach to cybersecurity that can effectively mitigate the risks posed by AI-augmented deepfake attacks.

1. Zero Trust Security Model:
SASE adopts a Zero Trust security model, which assumes that no user or device should be trusted by default, regardless of their location or network access. This approach helps prevent unauthorised access

[3] Gartner Predicts 30% of Enterprises Will Consider Identity Verification and Authentication Solutions Unreliable in Isolation Due to AI-Generated Deepfakes by 2026

to sensitive data and resources, reducing the likelihood of deepfake attacks infiltrating the organisation's network.

2. Secure Web Gateways:
SASE solutions include secure web gateways that can inspect and filter internet traffic in real-time, blocking malicious content such as deepfake videos or phishing attempts before they reach the end-users. This proactive approach enhances the organisation's defence against AI-augmented cyber threats.

3. Identity and Access Management:
SASE platforms offer robust identity and access management capabilities, allowing sports franchises to enforce strict authentication and authorization policies to ensure that only authorised users can access critical systems and data. This helps prevent unauthorised actors from exploiting vulnerabilities in the network.

4. Threat Intelligence and Analytics:
SASE solutions leverage advanced threat intelligence and analytics tools to detect and respond to suspicious activities, anomalies, or potential deepfake attacks in real-time. By continuously monitoring network traffic and user behaviour, sports organisations can proactively identify and neutralise cyber threats before they cause significant harm.

Mitigating Risk with Zero Trust

The Zero Trust security model employed by Secure Access Service Edge (SASE) plays a crucial role in preventing deepfake attacks on high-profile sports franchises by implementing a strict and proactive approach to network security. Here's how the Zero Trust security model helps in mitigating the risks of deepfake attacks:

1. No Implicit Trust:
The fundamental principle of Zero Trust is to trust no one and nothing by default, regardless of their location or network access. This means that every user, device, or application attempting to access the network resources of the sports franchise is treated as untrusted until proven otherwise. This approach eliminates the assumption of implicit trust, making it harder for malicious actors to infiltrate the network through deceptive means, such as deepfake content.

2. Identity Verification:
Zero Trust focuses on verifying the identity of users and devices before granting access to sensitive resources. By implementing strong authentication mechanisms, such as multi-factor authentication and biometric verification, high-profile sports franchises can ensure that only authorised individuals with legitimate credentials can access critical systems and data. This prevents unauthorised users, including AI-powered cybercriminals behind deepfake attacks, from gaining entry into the network.

3. Micro-Segmentation:
Zero Trust advocates for micro-segmentation, which involves dividing the network into smaller, isolated segments based on specific criteria, such as user roles, applications, or data types. By segmenting the network and enforcing strict access controls between segments, sports organisations can contain the spread of deepfake attacks and limit the impact of potential breaches. This granular approach to network

security reduces the attack surface and minimises the risk of lateral movement by cybercriminals leveraging deepfake techniques.

4. Continuous Monitoring and Inspection:
Zero Trust emphasises continuous monitoring and inspection of network traffic, user behaviour, and access patterns to detect anomalies and potential security threats in real-time. By leveraging advanced analytics and threat intelligence capabilities, high-profile sports franchises can proactively identify suspicious activities, such as the dissemination of deepfake content, and respond swiftly to mitigate the risks. This proactive stance enables organisations to stay one step ahead of cyber threats and prevent deepfake attacks from causing significant harm.

The Zero Trust security model embraced by SASE provides high-profile sports franchises with a robust defence mechanism against deepfake attacks by enforcing strict access controls, verifying user identities, segmenting the network, and continuously monitoring for potential threats. By adopting a Zero Trust approach, sports organisations can bolster their cybersecurity posture, safeguard their digital assets, and protect their reputation from the growing menace of AI-augmented cyber threats like deepfake attacks.

Mitigating risk with Cloud Access Security Broker (CASB)

CASB is a critical component of the Secure Access Service Edge (SASE) framework that helps in preventing deepfake attacks on high-profile sports franchises by enhancing cloud security and data protection. Here's how the CASB security model within SASE can mitigate the risks of deepfake attacks:

1. Visibility and Control:
CASB provides high-profile sports franchises with visibility into their cloud applications and services, allowing them to monitor user activities, data transfers, and access permissions. By gaining insights into cloud usage patterns, organisations can identify anomalous behaviour that may indicate the presence of deepfake attacks or unauthorised access attempts. CASB enables granular control over cloud access, ensuring that only authorised users can interact with sensitive data and applications, thereby reducing the risk of deepfake-related breaches.

2. Data Loss Prevention (DLP):
CASB solutions offer robust data loss prevention capabilities that help in identifying and protecting sensitive information from unauthorised disclosure or exfiltration. In the context of deepfake attacks, CASB can detect the unauthorised transfer of manipulated media files or confidential data, triggering alerts and enforcing policies to prevent data leakage. By implementing DLP controls, high-profile sports franchises can safeguard their valuable assets from being exploited by cybercriminals leveraging deepfake techniques.

3. Threat Detection and Response:
CASB platforms incorporate threat detection and response mechanisms that enable organisations to identify and mitigate security incidents in real-time. By analysing cloud traffic and user behaviour, CASB can detect suspicious activities associated with deepfake attacks, such as unauthorised access to cloud resources, abnormal data transfers, or malicious file uploads. Prompt detection and response to potential threats help in containing the impact of deepfake attacks and preventing further compromise of the organisation's cloud environment.

4. Compliance and Policy Enforcement:
CASB assists high-profile sports franchises in enforcing compliance with industry regulations and internal security policies related to data protection and access control. By defining and enforcing policies that govern the use of cloud applications, CASB ensures that data handling practices align with regulatory requirements and organisational guidelines. This proactive approach to compliance management reduces the likelihood of data breaches resulting from deepfake attacks and strengthens the overall security posture of the sports organisation.

The CASB security model within the SASE framework empowers high-profile sports franchises to secure their cloud environments, protect sensitive data, and mitigate the risks associated with deepfake attacks. By leveraging CASB's capabilities for visibility, data loss prevention, threat detection, and policy enforcement, sports organisations can enhance their resilience against AI-augmented cyber threats and safeguard their digital assets from malicious actors seeking to exploit vulnerabilities through deepfake techniques.

Conclusion:

In conclusion, the cybersecurity risks posed by AI-augmented deepfake attacks on high-profile global sports properties are real and evolving. By embracing Secure Access Service Edge (SASE) as a comprehensive cybersecurity solution, sports organisations can enhance their resilience against these sophisticated threats, safeguard their reputation, and protect their valuable data and content assets. With SASE's integrated approach to network security and access control, high-profile sports franchises can stay ahead of the curve and ensure a secure digital environment for their stakeholders, fans, and partners.

About the Author:

David Andrew
Founder & Managing Partner
www.tiaki.ai
david.andrew@tiaki.ai

David is the Founder & Managing Partner at TIAKI, a niche consulting practice helping executive leadership in sport make confident, informed decisions on their risks, investments and business outcomes powered by secure 'data-at-scale'.
He collaborates with bold and determined leaders in the sports ecosystem to define their data, AI and cybersecurity strategies to deliver sustainable value.

David's vision for TIAKI is to empower sports franchise CEOs, leadership teams, sports media broadcasters and investors in the global sports industry with strategic advisory frameworks to deliver secure, pioneering digital fan experiences and new ecosystem business models to achieve breakthrough returns.

David has over 20 years of strategy and technology enabled business transformation experience, providing consulting expertise in cloud native technologies, data strategy, digital business enablement and cybersecurity strategy. He is passionate about helping talented leadership teams succeed in securely growing their differentiated business models in the data-driven, digital sports economy.

Based in Stockholm, David previously worked for IBM Consulting, EY, Accenture Strategy and Orange Business. He studied Chemistry at Durham University and holds an MBA from Trinity College, Dublin Business School.