

Protecting Mobile Gambling Apps:

How XTD Defends Online Gambling,
Sports Betting, and Casino Industries and
Their Multitude of Players

CHAPTER 1

Online Gambling Makes a Popular Cyber Target

Online gambling is hot! From sports betting to poker, bingo, horse racing, lotteries, and more, millions of users worldwide enjoy modernized digital forms of gambling as entertainment. So much so that the global online gambling market value is projected to experience a compound annual growth rate of 11.7% and hit US\$153.57B by 2032.¹

Participating in online gambling requires users to provide their gambling platform of choice with sensitive personal information—name, address, credit card numbers, and even banking and other financial information. That data, combined with the skyrocketing number of players and huge amount of money involved, makes for a highly attractive ‘target market’ for bad actors looking to execute cyber attacks on gambling providers and their customers.

For instance, in June 2022 alone, 25% of all gambling sites were hit by ‘bookie bot’ distributed denial-of-service (DDoS) attacks perpetrated to disrupt or even take sites down.² In November, gambling company DraftKings suffered a credential-stuffing attack in which customers lost about \$300,000. DraftKings eventually refunded the loss, but its share price fell 5%.³ And as of January 2023, consumers had filed class-action lawsuits against BetMGM, LastPass, the San Francisco 49ers, JumpStart Games, Ethos Technologies, and Guidewire Software due to data breaches the plaintiffs claimed were caused by these companies’ negligence and poor cybersecurity practices.⁴

Among the many attack vectors that cybercriminals exploit, one of the most accessible is the gambling apps that customers use to engage in betting via their mobile devices. That makes securing those mobile apps critical for protecting customers and gambling companies alike.

¹ ResearchAndMarkets, Online Gambling Market Analysis Report 2023-2030

² Imperva Threat Research, 2022 Bad Bot Report

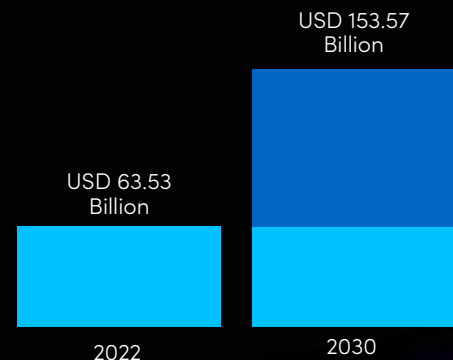
³ <https://www.cnn.com/2022/11/21/draftkings-says-no-evidence-systems-were-breach-following-report-of-a-hack.html>

⁴ <https://topclassactions.com/lawsuit-settlements/privacy/data-breach/data-breach-class-action-lawsuits-allege-company-negligence/>

Participating in online gambling requires users to provide their gambling platform of choice with sensitive personal information—name, address, credit card numbers, and even banking and other financial information.

Global Online Gambling Market

Market forecast to grow at CAGR of 11.7%



Source: Research & Markets

Common Cyber Threats to Online Gambling

Cyber attackers have a range of reasons and methods for targeting online gambling. The most obvious motivation is financial gain that can be achieved through direct theft and money laundering, fraud, identity theft, and disrupting services to shut out other players from accessing gambling sites (essentially gaming the game). But there can also be pride in gaining notoriety in this particularly high-profile domain. Some attacks even have political or hacktivist motivations from those living where gambling is considered immoral or even illegal.

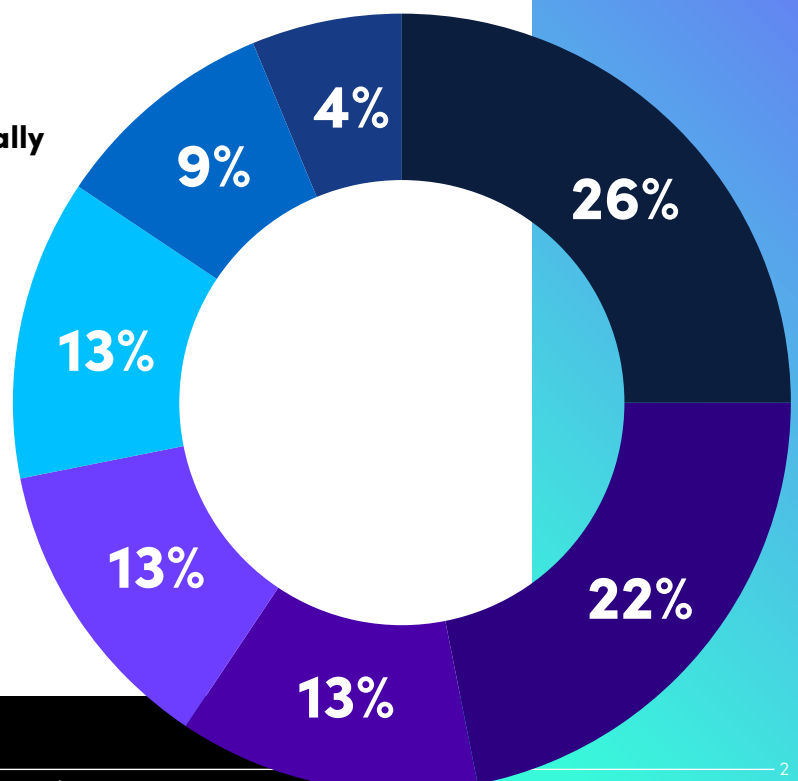
Some of the most common threats to online gambling include:

- › **Cross-site scripting.** This type of attack involves inserting some malicious code (often JavaScript) into a webpage, where it captures customers' information in real time while they are performing an action. The customer information is redirected to a server controlled by the attacker. Since this kind of attack directly affects customers who are transacting, there is great risk to a brand's reputation.
- › **API attacks.** Developers of online gambling apps regularly use Application Programming Interfaces (APIs) to integrate code that displays information like player line-ups, live scores, odds, statistics, and more. They may also use APIs to integrate betting odds into different websites, monitor betting lines, and streamline play. APIs, which often come from third-parties whose cybersecurity practices are lacking, can be used for stealing user data, gaining unauthorized system access, or disrupting a gambling service altogether.

Targetting of the sports sector globally (by campaign objective, 2017-22)

- Financial fraud
- Espionage
- Data theft
- Disruption
- Ransomware extortion
- Reconnaissance
- Cyber-enabled fraud

Source: UK National Cyber Security Centre



- › **Distributed Denial of Service (DDoS).** Bad actors may attempt to dominate a gambling platform (and its prize payouts) by flooding a site with traffic to shut out other users, make the platform unavailable, or even guide them to other black market sites. That's usually done by interrupting the hosting server. This type of attack can also be used as a means of distracting attention from other attacks happening at the same time. DDoS attack capabilities in a user-friendly format can even be rented, enabling almost anyone to launch an attack and force other players offline.
- › **Ransomware.** Hackers may trick users into clicking on malicious links or downloading malicious code, which then renders their data, or entire mobile device or computer, inaccessible until a ransom is paid. That may prevent players from collecting winnings, incentivizing them to pay up or suffer the loss. Similar attacks may be made against gambling companies' employees, whether on their laptops or mobile devices. Clicking on the wrong link can impact the user's device or even the company's other networked systems.
- › **Bad bots.** Automated bots are a growing mechanism for attacking online gambling sites. These automated software programs perform malicious tasks that enable attackers to steal user data, take over accounts, disrupt a gambling service, or otherwise manipulate the in-game environment. 55% of bot attacks in 2022 came from "simple" bots that, like DDoS attack code, can be bought online.⁵
- › **Data breaches.** Breaches of customer data compromise sensitive information, putting gambling companies at risk of non-compliance with laws and regulations and threatening their reputation in the market. In recent years, massive breaches at gambling companies like BetUS, William Hill, Clubillion, and others have led to the data exposure of hundreds of thousands of customers.



In recent years, massive breaches at gambling companies like BetUS, William Hill, Clubillion, and others have led to the data exposure of hundreds of thousands of customers.

⁵ Imperva Threat Research, Why Attackers Target the Gaming Industry

Mobile Apps Pose an Increasing Cyber Threat to Online Gambling

An online gambling company's most important asset is, of course, their customers. They engage with those customers via the mobile apps that are part of their business offerings. If the app or the connection between the app and the backend are compromised, there is a problem. Today, most applications are not protected. And as it's becoming more and more difficult for hackers to bypass security solutions in the enterprise, they look for alternatives—and apps offer the path.

There are several types of mobile app attacks that online gambling companies need to worry about:



A **Repackaging Attack** is where hackers take a legitimate online gambling app and modify it by adding malicious code or malware. The modified app is then repackaged and distributed through unofficial app stores or malicious websites, disguised as a legitimate download. When users unknowingly install these repackaged apps, they can compromise their device's security and expose personal information to cybercriminals.

Verimatrix XTD places multi-layered shields around the app, preventing attackers from reengineering or modifying it. Verimatrix XTD also reports repackaging attack attempts to our online gambling customers.



A **Screen Overlay Attack** is a type of mobile app cyberthreat where a malicious app displays an overlay on top of a legitimate online gambling app on a device. This deceptive technique tricks users into unknowingly granting sensitive permissions or interacting with fake interfaces, leading to potential data theft, unauthorized access, or fraudulent activities. By presenting an overlay that mimics the appearance of a trusted app or system prompt, attackers can manipulate users into providing sensitive information, such as login credentials or financial details. This type of attack capitalizes on the user's trust in the legitimate interface and their willingness to interact with it.

Verimatrix XTD identifies when overlay screens are triggered and data is sent to malicious servers. XTD alerts the app owner, and preventive or responsive countermeasures can be taken.



A **Supply Chain Attack** is a cyberthreat that targets the mobile development software supply chain to compromise the integrity or security of mobile applications. In this type of attack, attackers infiltrate the software development process by compromising a trusted and legitimate component or vendor involved in app development. By injecting malicious code or backdoors into the compromised component, the attacker gains unauthorized access to the mobile app's codebase, allowing them to manipulate or compromise the app's functionality or introduce vulnerabilities. When users download and install the affected app, they unknowingly expose their devices and data to potential harm. Supply chain attacks are particularly concerning as they can impact a large number of users and evade traditional security measures.

Verimatrix XTD detects app communications with blacklisted connections and provides these to our online gambling business customers. On the roadmap: Whitelist monitoring, whereby XTD alerts the app owner about unauthorized communications, identifying the backdoor and allowing app owners to respond.



An **Open-Source Vulnerability** refers to a cybersecurity risk found in mobile apps that utilizes open-source software components. Open-source software is publicly available and can be freely used by developers to build their applications. However, sometimes these open-source components may have security weaknesses or vulnerabilities that hackers can exploit.

Verimatrix XTD hardens apps using multi-layered security techniques such as obfuscation to prevent static and dynamic code analysis, mitigating open-source code exploitation risks. Essentially, XTD makes open-source app code difficult for an attacker to understand, thereby reducing the chance that open-source vulnerabilities will be exploited by attackers.



A **Payload Delivery Attack** is a cyberthreat where attackers try to deliver harmful software, called a payload, to a device through a malicious app or file. The payload can be malware or other malicious code that can harm the device or steal sensitive information. When users unknowingly download or install the malicious app or file, the payload is delivered, allowing hackers to gain control over the device or access the user's data. Think of the cyberattack as a cruise missile. The missile has two main parts: the rocket and the warhead. The rocket's purpose is to deliver the warhead to the target without being detected or intercepted. The warhead's job is to create damage. Often, a mobile app is the rocket and not the warhead. It helps deliver the attack to the right place without being detected or blocked. The rocket does not cause the damage, but without it, there is no attack.

Verimatrix XTD prevents payload delivery attacks by shielding the app from modification and infection. XTD detects connections from emulators and can immediately prevent the app from opening.



Geo-spoofing is a mobile app cyberthreat where attackers trick an online gambling app into believing it is located in a different geographic location than it actually is. They can use special techniques to manipulate GPS signals or network information to make it appear as if the device is in a different city, country, or even continent. Or they can use a VPN. This can lead to various risks, such as accessing geo-restricted content, evading location-based security measures, or engaging in fraudulent activities.

Verimatrix XTD detects VPN connections, as well as any banned locations specified by the customer, and can immediately block the app or even shut it down.

The Synopsis Cybersecurity Research Center security analysis of the 10 most popular Android sports and betting apps showed:

Downloads from Google Play Store:

> **21.5 mil**

Average number of components per app:

125

Average number of vulnerable components per app:

10

Average number of vulnerabilities per app:

179

Many apps in active development were using outdated open-source components with known vulnerabilities – a major cyber risk.

Source: CyRC special report: Secure apps? Don't bet on it

Key Impacts of Cyberattacks on Online Gambling Businesses

While technology is dramatically extending the reach of gambling enterprises, the widespread adoption of online gambling, especially involving mobile devices and apps, can also significantly impact the business and its customers. Depending on the severity and number of customers and assets involved, it may take weeks, months, or longer to overcome the potential impacts of a successful cyberattack.

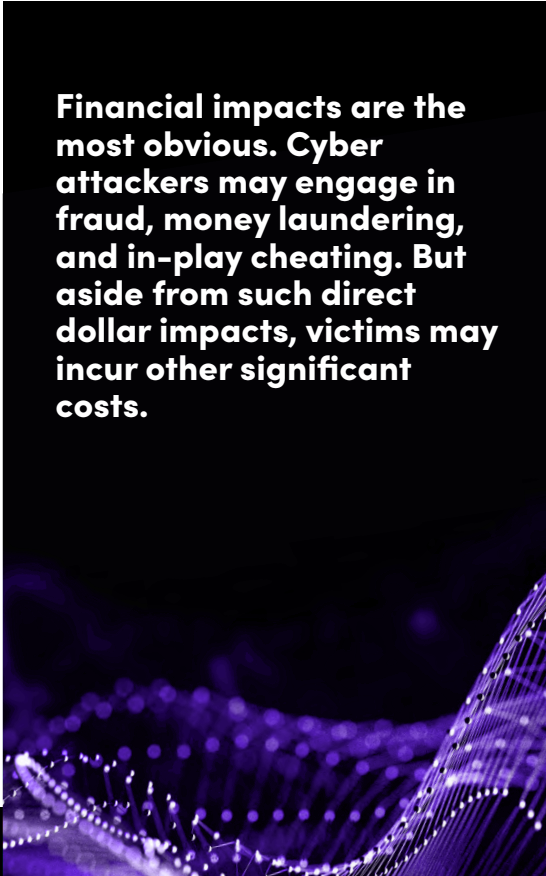
Financial impacts are the most obvious. Cyber attackers may engage in fraud, money laundering, and in-play cheating. But aside from such direct dollar impacts, victims may incur other significant costs. For example, in March 2020, sports betting solution provider SBTech was the victim of a ransomware attack that shut down their platform and affected hundreds of third-party websites that used it to run betting and casino services. The company set aside \$30M in escrow to cover damage and lost income as a result of the attack, and had to plan a payout of up to \$100M.

Cyberattacks can also impose other potential costs, like theft of intellectual property and trade secrets, and lost revenue from interruptions of normal business and gaming operations. Repairs to affected systems and networks may be needed, as well as a re-design of systems for collecting, processing, and storing customer data to keep it more secure.

User impacts are also a huge concern. Identity theft and the loss of personal funds are harmful to customers personally and will cause the business to lose the customer relationship. But cyber attackers may also go further with malicious actions like using unauthorized customer device access to launch phishing or business email compromise attacks.

Reputation, of course, is also a major consideration in the gambling sector. **Players must feel that play on a given site is fair and accurate and that the company that owns the site is trustworthy.** Cyberattacks that compromise customer data, payment methods, bank accounts, or privacy will cause reputational harm. Taking cybersecurity seriously and providing a secure playing experience will improve customer confidence that they are engaging with a trustworthy business.

Finally, there can be **regulatory** implications. Despite its popularity, gambling has always been a controversial cultural issue. There are many diverse regulations on different types of gambling activities across the US and around the world, many of which date back to before online gambling was ever invented. Cyberattacks can put a gambling company in violation of a number of regulations, with the modern twist of digital privacy being a big concern. It behooves the gambling industry to take cybersecurity seriously to preserve the regulatory gains that have been made and to convince regulators that online gambling is safe and can even be expanded.



Financial impacts are the most obvious. Cyber attackers may engage in fraud, money laundering, and in-play cheating. But aside from such direct dollar impacts, victims may incur other significant costs.

Technology Developments Shaping the Online Gambling Industry

Advances in technology are dramatically changing the online gambling landscape, offering new revenue opportunities for gambling companies and exciting new experiences for customers. As new technologies are adopted into mobile sportsbooks and other betting platforms, it's important to consider the cybersecurity implications up front and make these promising innovations as safe as possible.

Live Streaming



Thanks to advances in networking like 4G and 5G, players can now watch games on sportsbook websites in real-time and place wagers during live events. This is particularly good for events that don't get a lot of media coverage.

Virtual and Augmented Reality



VR and AR provide immersive experiences for players to feel the thrill of watching and betting on a live sport from wherever they are. Adding in sophisticated graphics to the VR and AR enhances the player experience even more, making this technology a very popular developing option for sportsbetting.

Mobile



Enabling mobile betting has been one of if not the most revolutionary changes the gambling industry has ever enjoyed. Bettors can access their favorite bookmaking sites, place bets, follow live gaming action and get instant results conveniently and, if they so choose, privately. Nearly every sportsbook and other legal form of gambling now offers a mobile app, and as we see in this paper, players are definitely taking advantage!

Blockchain and Cryptocurrency



Many online gambling sites, especially sportsbooks, have begun accepting cryptocurrencies for deposits and withdrawals. This digital currency offers customer an unprecedented level of anonymity and privacy, while also being very secure. Crypto's decentralized ledger system also reduces fraud and ensures winnings promptly reach the bettor.

Big Data



By collecting and analyzing massive amounts of data, online gambling companies can gain insights that were never before possible – such as team and player performance, customer preferences, and any number of factors that may positively or negatively affect the online and in-game experience.

CHAPTER 5

Traditional and New Laws Regulate Online Gambling

Gambling is subject to many regulations around the world, covering everything from data privacy to betting to payment processing. The dramatic increase in online gambling, especially accelerated during the COVID-19 pandemic when housebound people were looking for entertainment, caught many regulators a bit off guard, but they are now quickly catching up.

For instance, per industry experts at the International Masters of Gaming Law, the recent and rapid legalization of sports betting in many US states opened up huge new markets, with individual states taking slightly different regulatory approaches. While Latin American countries are moving towards liberalization in gambling regulation, European markets are erecting new regulatory barriers. As the industry evolves and cyberattacks increase, we can expect more changes and perhaps more enforcement of existing laws aimed at protecting customer data and finances. Just a few of the leading regulations include:

US Interstate Wire Act of 1961 (Federal Wire Act). The Act regulates online gaming, even though the internet didn't exist in the 1960s. To combat organized crime, the bill specifically prohibits the transmission (or "wiring") of information and payments regarding sports betting across state lines. A 2011 re-interpretation of the statute opened the door for other types of gambling to cross state lines, but sports betting was still prohibited, limiting the sports betting market's reach and pooling of players. Today, each state with legal sports betting must act independently, and players can only place [legal sports bets](#) with licensed providers in their state. There is currently a legal challenge to extend the law to limit any kind of cross-state gaming, which has yet to play out in the US court system.

2006 Unlawful Internet Gambling Enforcement Act (UIGEA). This law did not explicitly ban online gaming but prohibited US-based payment processors and other financial institutions from processing transactions involving online gaming services. The law forced many online gambling operators to move their businesses offshore.

As of 2023...

Only

7

US states have legalized online casinos.

5

more are considered likely to do so.

25

US states have legalized online sportsbetting.

International Gambling Laws are too numerous to mention. While some regions, like the Caribbean, are gambling-friendly, others, like China and multiple Arab countries, strictly oppose it. Even in places where it is legal, regulations for different forms of online gambling can vary widely.

Payment Card Industry Data Security Standard (PCI-DSS). This is a security standard for ensuring that all companies that accept, process, store, or transmit credit card information maintain a secure environment for that data. The intent is to improve payment account security throughout the transaction process. PCI-DSS is defined by the independent PCI Security Standards Council (SSC) but enforced by credit card companies.

General Data Protection Regulation (GDPR). Adopted in 2016 and enforced as of 2018, the GDPR is a European Union law protecting the personal data and privacy of European Economic Area (EEA) citizens. It applies to online gambling companies that sell to any of these citizens, regardless of where those companies are located worldwide. The GDPR sets firm rules for collecting, processing, and storing personal data by online gambling companies, and the EU is known to be quite strict on enforcement.

The GDPR sets firm rules for collecting, processing, and storing personal data by online gambling companies, and the EU is known to be quite strict on enforcement.






The Value of Extended Threat Defense Technology in Combatting Online Gambling Cyberattacks

The multitude of cyber-related challenges facing online gambling demand an elevated level of security to address the greatly increased risks in the modern environment of ubiquitous transacting. The current reality is that most mobile applications used by online gambling businesses are not well protected. Since it's becoming more and more difficult for hackers to bypass enterprise-level security solutions deployed by larger online gambling organizations, bad actors look for alternative entry vectors and discover the app path.

Extended Threat Defense (XTD) is the leading cybersecurity solution that secures online gambling businesses from risks originating from mobile applications. While many companies have some form of cybersecurity protection for employer-issued managed devices and personal “bring your own devices” (BYOD), XTD addresses multi-vector threats stemming from unmanaged (consumer) mobile devices like smartphones and tablets.

That specifically includes the range of multi-vector threats that previous cybersecurity solutions like mobile threat defense (MTD) and extended threat detection and response (EDR) miss.

 MTD	 XDR	 XTD
Provides real-time protection against threats and allows organizations to remotely manage and secure their mobile devices.	Provides continuous monitoring of endpoint devices and can detect and respond to a wide range of security threats, including malware, ransomware, and advanced persistent threats.	Helps prevent, detect, respond to and predict cyberattacks originating from the mobile app to the edge, and specifically multi-vector threats
Works on managed smart phones, laptops and tablets	Works on managed endpoint devices	Works on unmanaged devices; any device with an app
Requires an agent to be installed on the device – protects institution employees’ mobile devices, but is impractical for end customers	May take a more comprehensive security approach (continuous monitoring, incident response, and ability to identify and remediate vulnerabilities). Lacks integration, limiting visibility into the security posture and slowing response.	Uses behavioral analysis like EDR (for detection), combined with other EDR and MTD elements. Ideal when numerous unmanaged consumer devices are connected to an online gambling enterprise via the app

XTD monitors new entry vectors from the fastest-growing attack surface—connected apps, APIs, and unmanaged devices. That makes XTD an essential component of effective cyber defenses for online gambling businesses.

Polymorphic Protection: An Important App Security Attribute

An effective XTD platform should include polymorphic protective capabilities. This innovative approach involves constantly changing an application's code and structure to make it more challenging to hack. It's a bit like changing the password of your online accounts every so often to reduce your cyber vulnerability. Some savvy online gambling companies are already protecting their mobile apps with polymorphic protection.

Developers can use various techniques to make an app's code and structure more resistant to attack. One approach is to use obfuscation, which involves modifying the source, byte, or machine code so that it becomes significantly more difficult for hackers to read and understand. In essence, polymorphic protection transforms mobile apps into moving targets, making it much harder—even annoyingly complicated, if not nearly impossible—for hackers to reverse engineer code and develop malware that can penetrate the app's defenses.

That way, the code cannot be used to potentially reveal an app's inner workings or any exploitable vulnerabilities that may be found within it. Obfuscated code is also far less susceptible to tampering. Given the online gambling sector's particular vulnerability to cyberattacks, this approach is crucial for protecting customer information.

To implement polymorphic protection, online gambling businesses must invest in tools that not only shield mobile apps but also provide threat detection and response capabilities.



In essence, polymorphic protection transforms mobile apps into moving targets, making it much harder—even annoyingly complicated if not nearly impossible—for hackers to reverse engineer code and develop malware that can penetrate the app's defenses.

The Verimatrix XTD Approach

Verimatrix XTD offers an affordable and user-friendly solution that utilizes cutting-edge technology to secure mobile apps. With its ability to detect and respond to attacks promptly, Verimatrix XTD ensures the safety of mobile applications and prevents potential damage. Our military-grade, multi-layered security is very difficult for hackers to penetrate. We also help customers monitor the fastest-growing attack surface: consumer endpoints. By analyzing extensive data, Verimatrix XTD can predict future attacks and provide proactive protection.

Covering a Wider Attack Surface with Zero-Code Protection

Verimatrix XTD offers a truly distinct differentiator. Unlike those solutions that necessitate agent installation, Verimatrix XTD offers an agentless, zero-code approach. This capability enables the rich protection, attack detection, and response capabilities to be quickly and easily deployed without cumbersome development or coding—making speed to market a reality. This is especially valuable for the mobile transaction environment, where consumer devices with various levels of protection are always in play.

Addressing Multi-Vector Threats from Consumer Devices

Verimatrix XTD monitors and mitigates cyber threats originating from apps downloaded to unmanaged consumer devices. While many organizations implement cybersecurity measures for managed devices such as BYOD, Verimatrix XTD is one of the few solutions designed to address the multi-vector threats arising from unmanaged mobile devices. XTD can do this because its telemetry is built into its app protection and is automatically passed on to every app instance downloaded. That means any device using the app can be monitored, effectively expanding the coverage of the attack surface into new realms. With Verimatrix XTD, online gambling companies can secure a broader range of devices, providing comprehensive protection against potential threats.

With its ability to detect and respond to attacks promptly, Verimatrix XTD ensures the safety of mobile applications and prevents potential damage.

Verimatrix XTD offers an agentless, zero-code approach. This capability enables the rich protection, attack detection, and response capabilities to be quickly and easily deployed without cumbersome development or coding—making speed to market a reality.

With Verimatrix XTD, online gambling companies can secure a broader range of devices, providing comprehensive protection against potential threats.

Detecting and Responding to Active Attacks

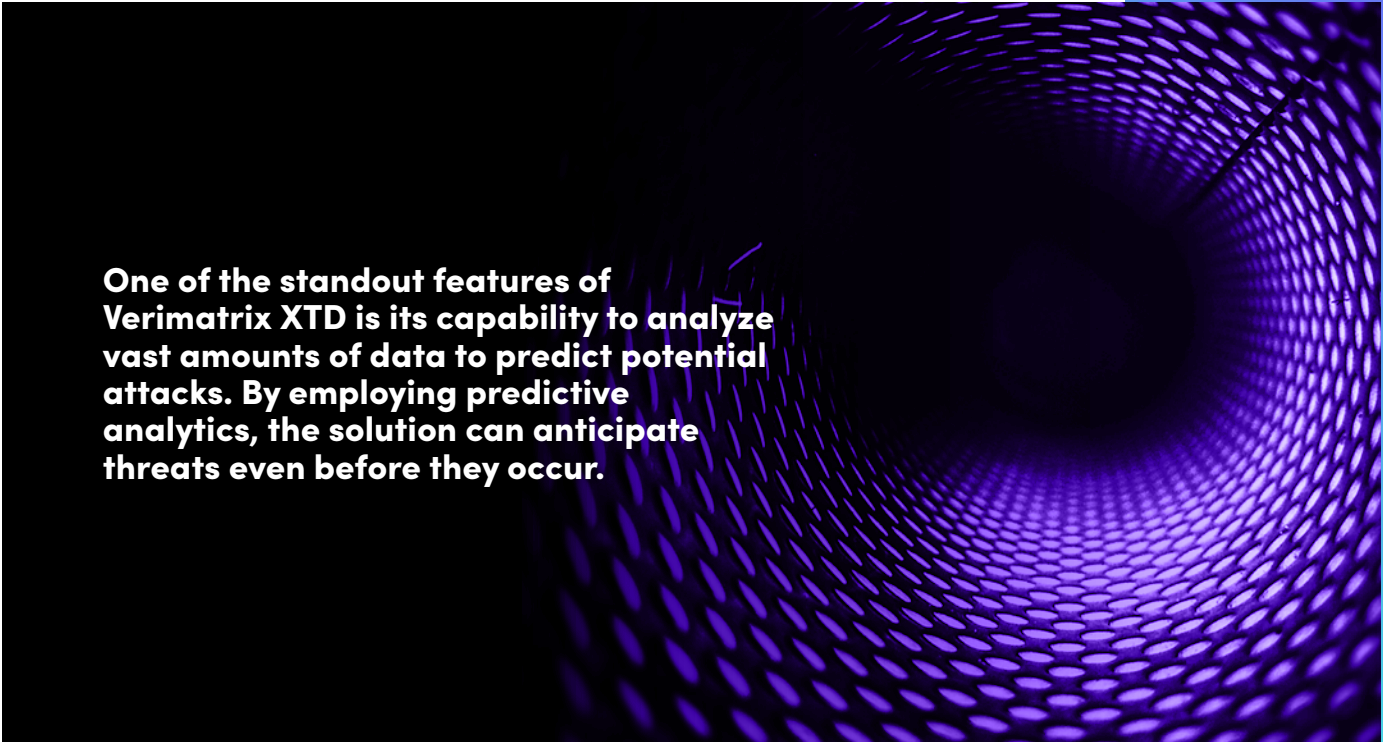
Verimatrix XTD's proactive defense strategy involves the swift detection of active attacks and an immediate response to neutralize potential damage. By leveraging advanced threat detection techniques, Verimatrix XTD identifies attacks in real-time, enabling security professionals to disconnect compromised devices promptly. This decisive action safeguards sensitive data and prevents malicious actors from exploiting vulnerabilities.

Proactive Protection through Predictive Analytics

One of the standout features of Verimatrix XTD is its capability to analyze vast amounts of data to predict potential attacks. By employing predictive analytics, the solution can anticipate threats even before they occur. This proactive approach empowers online gambling businesses to stay one step ahead of attackers, ensuring enhanced security for their mobile applications and connected infrastructure.

Understanding Risks and Empowering Security Professionals

Verimatrix XTD is dedicated to helping security professionals comprehend the risks associated with mobile applications and their connections. Highlighting the existence of blind spots by assigning a risk score to every threat found, Verimatrix XTD prompts online gambling businesses to acknowledge and address potential vulnerabilities. XTD provides security professionals with a meticulously designed Software-as-a-Service (SaaS) offering. There is also an optional service incorporating the services of human data scientists to review your account and take response actions on your behalf, adding an extra layer of expert assistance to combat evolving app threats effectively.



One of the standout features of Verimatrix XTD is its capability to analyze vast amounts of data to predict potential attacks. By employing predictive analytics, the solution can anticipate threats even before they occur.

Fight Back with Verimatrix XTD!

As the online gambling sector grows, so does the need for robust cybersecurity measures. Verimatrix XTD is an exceptional solution, providing affordable and user-friendly mobile app protection. With its agentless, zero-code approach, it allows for easy and painless deployment, allowing customers to monitor a wider attack surface, including unmanaged consumer devices.

Verimatrix XTD effectively detects active attacks and responds promptly, minimizing the potential for damage. By analyzing data and predicting attacks, it enables organizations to proactively protect their mobile applications. Armed with Verimatrix XTD's comprehensive security offerings and expert support, security professionals can effectively mitigate the risks associated with online gambling app vulnerabilities and secure their digital assets

Verimatrix – Award-winning Cybersecurity

Verimatrix helps power the modern connected world with security made for people. We protect digital content, applications, and devices with intuitive, people-centered, and frictionless security. We enable the trusted connections our customers depend on to deliver compelling content and experiences to millions of consumers around the world.

We are proud of the market recognition our innovative solutions have earned:



2023 Global Infosec Award for Hot Company in Mobile App Security – Cyber Defense Magazine



2023 Cybersecurity Excellence Awards – Gold Winner for Artificial Intelligence Security and Biggest Brand Growth



2023 Product of the Year, AI and Machine Learning – National Association of Broadcasters (NAB)



2022 Gartner® Hype Cycle™ for Application Security

[Get A Demo](#) of the Verimatrix XTD cloud-native platform, deployed in minutes to protect your apps!

Sources

<https://www.businesswire.com/news/home/20230330005372/en/Global-Online-Gambling-Market-Analysis-Report-2023-2030-Ease-of-Access-Through-Increased-Smartphone-and-Internet-Penetration-Bodes-well-for-the-Sector---ResearchAndMarkets.com>

<https://www.bitdefender.com/blog/hotforsecurity/data-leak-on-online-gambling-app-puts-millions-of-users-at-risk-of-cyber-attacks/>

<https://www.researchandmarkets.com/reports/5017642/online-gambling-market-size-share-and-trends>

<https://macsources.com/top-5-cybersecurity-breaches-in-online-gambling-industry/>

https://www.controlrisks.com/our-thinking/insights/cyber-threats-to-sport?utm_referrer=https://www.google.com

<https://cipher.com/cybersecurity-for-gambling/>

<https://eclipses.com/news/cyber-threats-of-online-gambling/>

<https://www.jdsupra.com/legalnews/the-importance-of-cybersecurity-in-the-7403859/>

<https://www.gambling.com/us/laws#:~:text=Internet%20casino%20gambling%20remains%20illegal,is%20technically%20breaking%20federal%20law>

<https://iclg.com/practice-areas/gambling-laws-and-regulations/1-opening-up-the-world-new-frontiers-new-opportunities>

<https://www.letsgambleusa.com/laws/>

<https://www.enterpriseappstoday.com/news/online-gaming-market-to-hit-usd-163-0-bn-globally-by-2032-at-10-2-cagr.html#:~:text=Market%20Overview&text=The%20global%20online%20gaming%20market,gaming%20market%20is%20mobile%20devices.>

<https://topclassactions.com/lawsuit-settlements/privacy/data-breach/data-breach-class-action-lawsuits-all-eg-company-negligence/>

<https://rapidapi.com/collection/sports-odds-betting-apis>

<https://www.synopsys.com/blogs/software-security/cyrc-special-report-gaming-apps-security-analysis/>

<https://worldpopulationreview.com/state-rankings/online-gambling-legal-states>

<https://sportsepreneur.com/sports-betting-industry-future-challenges-trends/>

<https://www.globalbrandsmagazine.com/key-technological-developments-in-the-sports-betting-industry/>

<https://www.jpost.com/special-content/top-technological-innovations-shaping-the-online-betting-industry-709888>

<https://www.cnbc.com/2022/11/21/draftkings-says-no-evidence-systems-were-breached-following-report-of-a-hack.html>