SentrySol Whitepaper

On-Device AI Behavioral Security for Web3 Mobile Version 1.0

Date: July 8, 2025

1. Executive Summary

The rapid growth of Web3 has exposed critical security vulnerabilities, particularly within the mobile ecosystem. Traditional security measures are insufficient against sophisticated threats like phishing, malicious smart contract calls, and zero-day social engineering. SentrySol introduces an AI-native, on-device behavioral security framework specifically designed to counteract these challenges in Web3 mobile environments, with an initial strategic focus on Solana Mobile Seeker. By continuously analyzing user behavior in real-time, SentrySol proactively detects and neutralizes threats, ensuring user trust and asset safety at the session level. This whitepaper details SentrySol's innovative approach, core functionalities, underlying technology, and strategic market positioning.

2. Introduction: The Web3 Mobile Security Imperative

The shift to Web3 promises unprecedented decentralization and user empowerment, aiming to put control in the hands of users through decentralized blockchains.[1] This new paradigm offers advantages such as data ownership, enhanced privacy, resilience against cyber threats, and broader inclusion in the global economy, fostering an open, trustless, and permissionless environment where data is visible to all participants and cannot be altered without network consensus.[3] However, this revolutionary shift also introduces novel attack vectors that exploit user trust and technical complexities. Mobile devices, serving as the primary gateway to Web3 for millions, are particularly susceptible due to their always-on nature and the intricacies of decentralized application (dApp) interactions. The decentralized nature of Web3 inherently shifts greater responsibility for security onto the individual user, making them a primary target for sophisticated attacks.[5]

Escalating Security Vulnerabilities in Web3 Mobile

The Web3 sector has experienced a dramatic increase in security incidents, resulting in significant financial losses and eroding confidence. In the first half of 2025 alone, Web3 security breaches led to nearly $2.5 billion in losses, a figure that surpassed the total losses of the previous year.[7] The year 2024 saw over $2.3 billion worth of cryptocurrency stolen across 760 incidents, representing a 31.6% increase in value compared to 2023.[1]

Among the various attack vectors, phishing has emerged as the most significant threat. It accounted for approximately $400 million in losses during the second quarter of 2025, representing half of the total losses for that period.[7] In 2024, phishing was responsible for $1.05 billion in losses across 296 incidents, nearly half of all value stolen that year.[1] Sophisticated phishing schemes, such as "FreeDrain," exploit tactics like SEO manipulation, free-tier web services, and layered redirection to trick users into submitting sensitive information like seed phrases to near-perfect clones of legitimate wallet services, leading to large-scale wallet draining.[8]

Another critical vulnerability is "blind signing," where users approve complex transactions without fully understanding their implications. The $1.5 billion Bybit hack starkly illustrated this risk, as hackers manipulated the platform's frontend, causing users to unknowingly approve fraudulent transactions presented as unreadable strings of code.[9] This vulnerability persists even with hardware wallets if the transaction preview itself is compromised, revealing a critical gap in security *before* the final signature is made.[9]

Malicious smart contract calls also pose a substantial threat. Vulnerabilities within dApps or wallet interfaces can be exploited, leading to significant fund losses and undermining the credibility of protocols.[11] Common smart contract vulnerabilities include reentrancy attacks, front-running, integer overflow/underflow, and unchecked external calls.[11] For instance, Euler Finance experienced a $197 million loss due to a flash loan attack that exploited a smart contract vulnerability.[11]

Furthermore, zero-day social engineering attacks, which are new and unpredictable human-centric exploits, are particularly difficult for static analysis to detect. Attackers often "play the long game" by building rapport with targets or directly impersonating prominent figures, companies, or websites to gain trust before executing their malicious schemes.[13]

The Solana ecosystem, a key focus for SentrySol, has also faced its share of security challenges. It has experienced application-level exploits, supply chain attacks, and core protocol vulnerabilities.[14] Notable incidents include the Wormhole Bridge exploit in February 2022, which resulted in a $325 million loss due to a signature verification flaw, and the Slope Mobile Wallet exploit. These incidents frequently involve flaws in the design, coding, or configuration of dApps, wallets, or DeFi protocols, leading to unauthorized access, fund theft, or manipulation of operations.[14]

Impact on User Trust and Web3 Adoption

These escalating threats culminate in significant risks like wallet draining and address spoofing, which severely erode user confidence and impede the broader adoption of Web3 technologies. Critics view Web3 as a "breeding ground for unregulated crime" and "get-rich-quick Ponzi schemes" that can harm vulnerable consumers.[2]

User concern over security is a primary barrier to mainstream Web3 adoption. A significant portion of users, 44%, manage multiple wallets for safety, and 18% identify security as their top issue with wallets. More than half of users express a desire for wallets and dApps to provide more proactive protection.[16] This demonstrates a direct link between security incidents and the willingness of users to engage with decentralized technologies. If Web3 technologies are not intentionally designed to natively protect users, exploitation and abuse will persist, hindering the ecosystem from reaching a mature state and critical mass of user adoption.[2]

The increasing prevalence of phishing and blind signing attacks highlights a fundamental shift in attacker strategies. Instead of solely focusing on underlying protocol vulnerabilities or private key compromises, malicious actors are increasingly targeting the human element within the Web3 ecosystem. This means that security solutions must evolve beyond traditional code audits or network perimeter defenses to incorporate intelligent, real-time behavioral analysis that can discern genuine user intent from deceptive manipulation. SentrySol's focus on "behavioral security" and "user intent" directly addresses this evolving threat landscape. The billions in financial losses and the explicit concerns expressed by users establish a clear causal link: a lack of perceived security erodes trust, which in turn prevents the widespread adoption that Web3 advocates envision. SentrySol's mission of "ensuring user trust and asset safety" is therefore not merely a feature, but a foundational requirement for the entire Web3 ecosystem to achieve its promised potential and move beyond early adopters. While hardware wallets and Trusted Execution Environments (TEEs) like SeedVault secure the final signing process and private keys, the Bybit hack and similar incidents demonstrate that even with secure signing mechanisms, if a user is tricked into initiating a malicious transaction due to a compromised frontend or deceptive prompt, the hardware wallet cannot prevent the *intent* to sign. This reveals a critical security gap that exists *before* the final signature is made. SentrySol's focus on "pre-signing intelligence" and "analyzing user behavior...before fraudulent transactions occur" directly addresses this nuanced, yet critical, vulnerability, acting as an intelligent guardian during the dApp session that complements, rather than competes with, hardware-level key security.

SentrySol directly addresses these critical security deficiencies, moving beyond reactive detection to proactive, intelligent threat neutralization. The scale of the problem is evident in the following figures:

Table 1: Web3 Mobile Security Incident Trends (2024-2025)

Metric	H1 2025 (CertiK) [7]	2024 (CertiK) [1]
Total Losses (USD)	~$2.5 Billion	>$2.3 Billion
Net Losses (USD)	~$2.29 Billion	N/A
Number of Incidents	N/A	760
Average Loss per Incident (USD)	N/A	$3.1 Million
Losses by Attack Vector (USD)		
Phishing	~$400 Million (Q2)	$1.05 Billion
Private Key Compromise	Decreased	$855.4 Million
Code Vulnerabilities	Historical Averages	N/A

3. The SentrySol Solution: AI-Native, On-Device Behavioral Security

SentrySol operates as a silent, intelligent guardian, continuously analyzing user behavior to identify and neutralize threats before fraudulent transactions occur. The framework is built on the premise that genuine user intent has a unique behavioral fingerprint, and deviations from this pattern signify danger.

3.1 Core Purpose & Problem Solved

SentrySol preserves and reinforces user trust by providing a robust, real-time security layer that intercepts fraudulent transactions. It protects users from several critical attack vectors:

- **Phishing prompts and deceptive signing modals:** SentrySol detects subtle anomalies in user interaction and wallet signing behavior. AI-driven phishing detection systems analyze the context, linguistic patterns, URLs, and overall user behavior to identify potential red flags and inconsistencies indicative of a phishing attempt.[17]
- **Invisible malicious contract calls:** The system analyzes dApp interaction flows for suspicious patterns and hidden intents. This capability directly addresses common smart contract vulnerabilities such as reentrancy attacks, front-running, integer overflows, and unchecked external calls, which can lead to significant fund draining and compromise protocol integrity.[11]
- **App-side logic exploits and zero-day social engineering:** SentrySol provides adaptive, AI-enhanced protection that learns and responds to novel threats directly on the device. Behavioral biometrics continuously verify user identity by analyzing unique patterns of interaction with devices, detecting unusual behavior that may indicate fraud or coercion, even when traditional authentication methods are bypassed.[19]
- **Wallet Draining & Address Spoofing:** SentrySol's analysis of user intent and transaction context is specifically designed to flag and prevent attempts to gain unauthorized control over or redirect user funds. This counters sophisticated drainer scams that generate malicious approve() or permit() data to gain unlimited access to user tokens, and it provides an additional layer of verification against address spoofing, which can bypass simple visual inspection by using purely numerical addresses.[13]

3.2 Key Features & Functionality

SentrySol integrates several sophisticated components to deliver comprehensive protection:

3.2.1 Federated Anomaly Detection Engine

This engine utilizes lightweight, TinyML-compatible AI models, including transformers for sequential behavior analysis and Graph Neural Networks (GNNs) for analyzing dApp interaction flows and transaction relationships. These models are trained on user and device session signals to build a baseline of "normal" behavior and identify statistically significant deviations indicative of malicious activity.

The choice of **TinyML** is strategic, enabling machine learning directly on resource-constrained mobile devices. This approach significantly cuts down latency by handling data straight on the device, eliminating network delays and data transfer overhead that can account for 25-30% of processing time.[21] It also enhances privacy by ensuring that raw user behavioral data never leaves the device, keeping sensitive information within the device's secure enclave and aligning with data protection regulations like GDPR.[21] TinyML excels in real-time anomaly detection, with reported accuracies as high as 99.80%.[25] To optimize for mobile hardware, SentrySol employs model compression techniques such as quantization, which reduces the precision of numbers in the model, and pruning, which selectively eliminates redundant connections within the neural network architecture without significantly compromising accuracy.[26] This ensures that the advanced security features do not negatively impact device performance or battery life.

Transformers, originally developed for natural language processing, are highly effective for anomaly detection in sequential data. They leverage self-attention mechanisms to capture long-term dependencies and contextual relationships within user activity logs and behavioral patterns.[29] This allows SentrySol to model both periodic user behaviors (e.g., daily login patterns) and irregular anomalies (e.g., brute force attacks) with high accuracy and efficiency.[29]

Graph Neural Networks (GNNs) are particularly suited for analyzing complex relationships within networks by operating on graph-structured data.[36] In the context of Web3, GNNs can model blockchain transactions where nodes represent entities such as users, smart contracts, or wallets, and edges signify the interactions or transactions between them.[38] GNNs excel at detecting financial fraud by analyzing how transactions are connected, uncovering suspicious patterns across the entire network that traditional models, which examine individual transactions in isolation, might miss.[40] For dApp interactions, GNNs can identify deviations such as unusually high transaction volumes, rare interaction sequences, or connections to addresses previously identified as malicious.[37] This allows SentrySol to build a rich understanding of normal interaction and transaction patterns through a process called message passing, where nodes learn from their neighbors.[37]

The combination of TinyML for efficiency, Transformers for sequential analysis, and GNNs for relational data forms a synergistic architecture. Each component addresses a specific aspect of behavioral analysis, together creating a robust and dynamic "behavioral fingerprint of intent." This multi-modal AI approach enables SentrySol to detect subtle, multi-faceted anomalies that single-model or single-data-type solutions would likely miss, significantly enhancing its ability to combat sophisticated, evolving threats that blend technical exploits with social engineering.

3.2.2 Real-time User Behavior Monitor

This component continuously observes various behavioral signals to construct a dynamic profile of normal user interaction. This includes:

- **Transaction Timing:** Analyzing the speed and pauses in user approval sequences. AI-powered fraud detection systems incorporate transaction timing as a crucial feature to predict suspicious activity, flagging transactions occurring at unusual hours or with abnormal speeds.[41]
- **Touch Cadence & Gestures:** Recognizing patterns in physical interaction with the device screen. Behavioral biometrics track subtle patterns such as typing speed, rhythm, pressure, mouse/touch movement speed, direction, acceleration, and scrolling behavior to identify unique user interaction styles.[20] Deep learning models are increasingly used for motion recognition and anomaly detection based on sensor data, allowing for the identification of deviations from typical user movements.[43]
- **dApp Interaction Sequences:** Mapping the typical flow of user engagement within decentralized applications. AI-driven behavioral systems continuously monitor users throughout their session, reducing the risk of session hijacking and unauthorized access by identifying deviations from learned normal decision-making sequences.[45]
- **Wallet Signing Behavior:** Monitoring the context and frequency of signature requests to detect anomalies.

3.2.3 Signature Validator and Phishing Interceptor

This component is crucial for preventing "blind signing". It contextually validates signature requests by:

- **Cross-referencing User Intent:** Comparing the observed user behavior (e.g., what buttons were pressed, what was displayed) with the actual payload being requested for signature. Solutions like Human Wallet aim to provide plain-language transaction previews on tamper-proof screens of hardware wallets, while Liminal's solution displays human-readable transaction data for EVM chains, allowing users to cross-verify what they are approving.[9]

- **Analyzing Transaction Context:** Understanding the dApp, the typical transaction types, and the requested permissions to identify any discrepancies.
- **Active Prevention:** If a mismatch or malicious intent is detected, SentrySol actively prevents the payload from being signed and alerts the user, effectively blocking fraudulent transactions before they are executed. This capability is akin to advanced AI phishing detection systems that can block malicious emails before they reach the recipient's inbox.[18]

3.2.4 Trusted Execution Environment (TEE) Interface

SentrySol deeply integrates with secure hardware enclaves like Solana Mobile's SeedVault. This integration provides:

- **Hardware-Level Protection:** Critical security operations and sensitive data, such as derived cryptographic keys for behavioral models, are performed within a tamper-proof environment. TEEs are secure areas of the main processor that ensure the confidentiality and integrity of code and data loaded within them, protecting against software attacks originating from the Rich Operating System (Rich OS).[48]
- **Enhanced Key Security:** While SeedVault primarily protects private keys by moving them to the highest privileged environment available on the device, ensuring they never leave the secure execution environment [50], SentrySol leverages the TEE for its own operational security. This makes SentrySol highly resistant to sophisticated software attacks, providing a robust layer of defense for its internal processes.
- **Secure AI Model Inference:** TEEs are increasingly recognized for their ability to provide a secure environment for AI model inference, protecting against unauthorized access and data breaches.[52] They ensure the integrity of AI models and protect intermediate states, preventing private data leakage during computation.[54] This deep integration means SentrySol's AI decisions are themselves tamper-proof and trustworthy, even if the main operating system is compromised. This level of hardware-backed AI integrity establishes a "trusted AI" paradigm on the device, which is critical for building user confidence in autonomous security decisions.

SentrySol's emphasis on "proactive" and "real-time" prevention before a transaction is signed represents a fundamental shift from traditional, reactive security measures. In Web3, where transactions are often irreversible, preventing malicious actions *before* they occur is paramount to minimizing financial losses and user distress. This proactive stance directly addresses the pain points of wallet draining and blind signing, which have plagued the ecosystem.

Table 2: SentrySol's Core Technology Components & Benefits

Component	Key Function	Primary Benefit
Federated Anomaly Detection Engine	On-device anomaly detection, sequential behavior analysis (Transformers), graph-based threat detection (GNNs)	Resource efficiency, real-time threat adaptation, detection of complex fraud networks
Real-time User Behavior Monitor	Continuous behavioral profiling (transaction timing, touch cadence, dApp sequences, wallet signing)	Proactive threat neutralization, adaptive security measures
Signature Validator & Phishing Interceptor	Contextual signature validation, cross-referencing user intent with payload	Protection against blind signing, active prevention of fraudulent transactions
Trusted Execution Environment (TEE) Interface	Hardware-backed security for critical operations and sensitive data (e.g., derived cryptographic keys, model parameters)	Tamper-proof AI decisions, enhanced key security, resistance to sophisticated software attacks

4. Technology Approach: AI-Native, On-Device, Privacy-Preserving

SentrySol's technological foundation is built on three core pillars: AI-Native and On-Device Processing, Privacy-Preserving Federated Learning, and Hardware-Level Security. These pillars collectively ensure a robust, efficient, and user-centric security solution for the Web3 mobile ecosystem.

4.1 AI-Native and On-Device Processing

All SentrySol AI models and processing occur entirely on the mobile device. This approach offers significant advantages that are crucial for Web3 mobile security:

- **Minimal Latency:** Real-time threat detection is achieved without the delays inherent in network communication. On-device AI processing significantly reduces latency by eliminating both data transfer overhead, which can account for 25-30% of processing time, and network latency, adding an extra 15-20% delay when relying on cloud processing.[21] This ensures immediate responses critical for time-sensitive security applications.

- **Enhanced Privacy:** A fundamental advantage is that no raw user behavioral data ever leaves the device, ensuring superior data sovereignty. Sensitive data collected by modern device sensors—such as accelerometers, gyroscopes, and biometric sensors—is safeguarded within the device's secure enclave by on-device AI processing, guarding against misuse and unauthorized access.[21] This approach aligns strongly with stringent data protection regulations like GDPR, as it minimizes the risk of data leaks.[22]
- **Continuous Protection:** Security remains active even when the device is offline or has an unstable network connection, providing uninterrupted defense against threats.[22]
- **Resource Efficiency:** SentrySol leverages lightweight TinyML models, optimizing for mobile hardware constraints. TinyML is specifically designed to run machine learning models on ultra-low-power devices like microcontrollers, consuming milliwatts or less of power. This reduces energy demands, extends device lifespans, and minimizes maintenance needs.[22] Model compression techniques, such as quantization and pruning, are employed to reduce model size and inference time without significant compromise to accuracy, ensuring that advanced security features do not burden device performance or battery life.[26] This deliberate engineering effort makes the solution practically viable and scalable for real-world mobile deployment.

4.2 Privacy-Preserving Federated Learning

SentrySol's AI models continuously adapt to new and evolving threats. This learning process is achieved through Federated Learning, ensuring privacy.

- **Decentralized Training:** AI model improvements occur by sharing only aggregated gradient metadata, not raw user data, from devices.[24] This approach eliminates the need for centralized data aggregation, which is particularly critical for maintaining privacy and compliance in environments handling sensitive data.[56]
- **Collaborative Intelligence:** The system collectively learns from global threat patterns while strictly maintaining individual user privacy.[56] Privacy-enhancing techniques such as differential privacy, which introduces statistical noise to model updates, and secure aggregation, which uses cryptographic protocols to allow the server to compute the sum of encrypted updates without seeing individual contributions, further mitigate the leakage of sensitive information.[24] Federated

Learning is not merely a privacy feature; it is a critical enabler for the *adaptability* and *long-term efficacy* of SentrySol's on-device AI. It allows the models to learn collaboratively from global threat patterns without compromising individual user privacy, ensuring the system can proactively identify and respond to emerging attack techniques across its user base.

4.3 Hardware-Level Security

Deep integration with Trusted Execution Environments (TEEs) provides a robust, tamper-proof environment essential for safeguarding sensitive security operations and model parameters.

TEEs are secure areas of the main processor that isolate trusted applications and their data from the Rich OS, protecting the execution of authenticated code, confidentiality, authenticity, privacy, and system integrity.[48] This hardware-backed security makes SentrySol highly resilient against even the most sophisticated malware and root exploits, forming a foundational layer of trust for the AI's decisions. TEEs are increasingly used for secure AI model inference, protecting AI models from unauthorized access and ensuring their integrity during execution.[52] The emphasis on "no raw user behavioral data ever leaves the device," "superior data sovereignty," and compliance with regulations like GDPR positions SentrySol as a solution built with privacy as a core design principle. This strong alignment with the core values of the Web3 movement, which champions user control and data ownership, provides a significant competitive advantage and is expected to foster greater user trust and accelerate adoption.

5. Target Market & Use Cases

SentrySol targets the rapidly expanding mobile security layer within the Web3 ecosystem, a market projected to reach multi-billion dollar valuations. The growth in Web3, dApp, and crypto wallet markets directly fuels an urgent and expanding demand for specialized security solutions like SentrySol.

5.1 Primary Audience

SentrySol is strategically positioned to serve several key segments within the Web3 mobile landscape:

- **Solana Mobile Seeker Users:** As the initial strategic focus, SentrySol provides native, enhanced dApp security directly integrated with the device. The Solana Seeker has already garnered significant interest, with over 140,000 units sold through presales across 57 countries before its scheduled 2025 release.[57] The device features a new Seed Vault, a hardware-based security system designed to protect users' sensitive crypto assets by keeping keys, seeds, and secrets within a secure execution environment.[51]

- **Web3 Wallet Providers:** SentrySol offers Software Development Kits (SDKs) for seamless integration, enabling wallet providers to bolster their wallet's intrinsic security layers with SentrySol's behavioral intelligence. The global crypto wallet market was estimated at USD 12.59 billion in 2024 and is projected to reach USD 100.77 billion by 2033, growing at a Compound Annual Growth Rate (CAGR) of 26.3% from 2025 to 2033.[60] Mobile wallets, in particular, have been instrumental in driving mass adoption.[61] Wallet providers face significant security challenges related to the self-custody of keys and the immutability of smart contracts, where a single overlooked bug can lead to substantial losses.[6]
- **dApp Developers:** SentrySol provides tools and guidelines to embed advanced security directly into their decentralized applications, fostering a safer user experience. The market for decentralized applications (dApps) is projected to be worth USD 368.25 billion by 2027, with a rapid CAGR of 56.1%. In 2024, there were 24.6 million daily dApp users, with DeFi being the most dominant sector.[62] dApp developers contend with security challenges stemming from open-source code vulnerabilities, the potential for data breaches when linked to centralized storage, and human error.[64] They also face the imperative to establish robust user identification and Know Your Customer (KYC) mechanisms to comply with regulations, as failure to comply can lead to significant penalties.[65]
- **Mobile OEMs (Original Equipment Manufacturers):** SentrySol seeks partnerships for white-label solutions to pre-install SentrySol as a foundational, always-on security layer on Web3-native smartphones. Several OEMs are already developing Web3 phones with built-in security features, such as hardware-based seed vaults, secure enclaves, and biometric authentication (e.g., Solana Seeker, Samsung Galaxy Crypto Edition, Vertu Metavertu).[66] The market for white-label mobile security solutions is growing, indicating a readiness among manufacturers to integrate specialized security features directly into their devices.[68]

This multi-pronged audience strategy positions SentrySol to become a foundational security layer across the entire Web3 mobile ecosystem. The interest from OEMs in "Web3 phones" and "white-label solutions" suggests a significant opportunity for SentrySol to be pre-installed or deeply integrated into the hardware itself. This widespread integration would not only drive SentrySol's adoption but also elevate the overall security posture of the Web3 mobile space, fostering greater trust and accelerating mainstream adoption of decentralized technologies. SentrySol thus becomes an essential piece of the infrastructure, not merely an add-on.

5.2 Key Use Cases

SentrySol's capabilities address critical security needs across various Web3 interactions:

- **Preventing Blind Signing:** SentrySol ensures users are fully aware of what they approve, directly addressing the vulnerability exploited in major incidents like the Bybit hack.[9]
- **Securing DeFi Interactions:** It protects complex swaps, liquidity provisions, and lending/borrowing activities from exploitation. This is crucial given the significant value locked in DeFi, which reached $214 billion in 2024, and the prevalence of smart contract exploits that can lead to substantial losses.[11]
- **Protecting NFT Transactions:** SentrySol safeguards mints, trades, and transfers from phishing and malicious contracts. While NFT trading volumes saw a decline in 2024, the market is broadly expected to expand, increasing the need for robust protection.[62]
- **Mitigating Wallet Draining:** The solution intercepts fraudulent transactions designed to empty a user's wallet, directly countering sophisticated phishing scams like "FreeDrain" that trick users into compromising their assets.[8]
- **Combating Address Spoofing:** SentrySol provides an additional layer of verification beyond visual inspection for recipient addresses, addressing the tactic where malicious actors use purely numerical addresses to bypass readable transaction data.[13]
- **On-Chain Forensics Contribution:** Beyond immediate prevention, SentrySol contributes valuable real-time behavioral data and threat intelligence for post-incident analysis and broader ecosystem security. AI-driven threat intelligence can identify patterns of coordinated attacks and trace malicious offenses, aiding in the understanding and mitigation of future threats.[39] The inclusion of "On-Chain Forensics Contribution" as a key use case is noteworthy. This implies that the rich behavioral data and threat intelligence gathered on-device can also be valuable for post-incident analysis, tracing attack patterns, and improving broader ecosystem security. This extends SentrySol's value proposition beyond immediate protection to contributing to the collective security intelligence of the Web3 space, potentially fostering partnerships with security firms and regulatory bodies interested in combating illicit activities.

The following table illustrates the significant growth projections for SentrySol's target markets:

Table 3: Web3 Mobile Market & Wallet Growth Projections

Market Segment	2024 Market Size (USD Billion)	Projected Market Size (USD Billion)	CAGR (Forecast Period)	Key Drivers
Global Web3 Market	$8.4 (2024) [61]	$81.5 (by 2030) [75] / $68.8 (by 2033) [61]	43.7% (2025-2030) [75] / 23.7% (2025-2033) [61]	Increased transparency, high data security, NFTs, R&D investment, AI integration, 5G adoption [75]
Global dApp Market	N/A (24.6M daily UAW) [63]	$368.25 (by 2027) [62]	56.1% (CAGR) [62]	Decentralized finance (DeFi), gaming, NFTs, user empowerment [62]
Global Crypto Wallet Market	$12.59 (2024) [60]	$100.77 (by 2033) [60]	26.3% (2025-2033) [60]	Widespread crypto adoption, DeFi popularity, NFTs, demand for secure, user-friendly solutions, mobile wallets [60]

6. Competitive Positioning

SentrySol carves a unique niche by converging on-device, AI-native behavioral analysis with deep hardware integration, specifically tailored for the dynamic threat landscape of Web3 mobile. This approach represents a new paradigm in Web3 mobile security, moving beyond traditional reactive measures to offer a proactive, intelligent, and user-aligned defense against the unique and evolving threats of the decentralized world.

Differentiation from General Antivirus (e.g., Kaspersky)

General antivirus solutions, such as Kaspersky, offer broad malware detection and system protection across various operating systems like Windows, macOS, Android, and iOS.[76] While effective against general malware and online threats, these solutions are not specialized for the unique behaviors, transaction contexts, and intricate smart contract interactions inherent to Web3.[76] SentrySol's advantage lies in its specific focus on the nuanced, human-centric attack vectors prevalent in Web3 mobile environments, going beyond generic malware detection to understand and counter the specific deceptive tactics used in decentralized applications.

Distinction from Device Security Platforms (e.g., Samsung Knox)

Device security platforms like Samsung Knox provide robust hardware-level operating system security, safeguarding sensitive credentials such as passwords, PINs, and biometrics in physically isolated environments.[77] They offer features like Auto Blocker for unauthorized app installs and aim to protect the core OS. However, while Knox secures the underlying operating system, it does not inherently focus on intelligent behavioral protection within Web3 interactions. SentrySol builds on top of this foundational hardware security by providing a crucial

application-layer defense specifically for dApp and wallet interactions, covering security aspects that general OS security typically does not address.

Contrast with Cloud-Based Web3 Security Solutions (e.g., Fireblocks, Zengo, Certik)

Cloud-based Web3 security solutions, such as Fireblocks and Zengo, utilize advanced cryptographic techniques like Multi-Party Computation (MPC) and secure enclaves for key management and transaction authorization.[79] Certik primarily offers code security audits, penetration testing, and compliance services, which are typically performed pre-deployment or for post-incident analysis.[83] While these solutions offer valuable services, they often involve a server-side component for key shares, aggregation, or analysis, which can introduce latency and privacy considerations.[79] SentrySol's fully on-device operation ensures unparalleled privacy and continuous protection, contrasting sharply with solutions that rely on centralized servers for analysis. This minimizes raw data exposure and ensures security remains active even when the device is offline or has an unstable network connection.[21] The repeated emphasis on "on-device," "no raw data leaves the device," and "continuous protection even offline" is not just a technical feature but a strong competitive differentiator. Cloud-based solutions inherently face latency and privacy trade-offs, which SentrySol's architecture avoids, creating a significant competitive advantage and aligning perfectly with Web3's decentralized ethos.

Complementary Role with Hardware Wallets (e.g., Ledger, Solana SeedVault)

Hardware wallets, such as Ledger and Solana's SeedVault, are designed to secure the final signing process and private keys by keeping them offline or within a Trusted Execution Environment (TEE).[50] They are critical for robust key custody. However, a common perception is that hardware wallets provide ultimate security. Yet, incidents like the Bybit hack demonstrate that even with secure hardware, if the user is

deceived by a malicious frontend into initiating a fraudulent transaction, the hardware wallet's role is limited to securely signing what it is presented.[9] It does not inherently prevent the

user's intent from being manipulated. This highlights a critical "blind spot" in the current security landscape. SentrySol fills this crucial, previously unaddressed gap by providing intelligent, real-time behavioral analysis *during the dApp session*, *before* a transaction even reaches the final signing stage. This adds a critical layer of *pre-signing intelligence* that actively prevents "blind signing" and user manipulation, a vulnerability that hardware wallets alone cannot fully address.

Different from Auditing Firms (e.g., 8kSec, Certik)

Auditing firms, such as Certik, specialize in providing pre-deployment static analysis of smart contracts and code, identifying vulnerabilities before a dApp goes live.[64] While essential for initial code integrity, this approach does not account for dynamic, real-time threats or user-centric exploits that emerge post-deployment. SentrySol, in contrast, offers dynamic, real-time runtime protection against live, evolving threats and user-centric exploits that static analysis might miss. This means SentrySol complements the work of auditing firms by providing continuous vigilance against threats that manifest during actual user interaction.

By differentiating itself from general antivirus (OS-level), device security platforms (OS-level), cloud-based Web3 security (off-device/centralized), hardware wallets (final signing), and auditing firms (pre-deployment), SentrySol positions itself as a unique, comprehensive solution. It does not replace these existing security layers but rather complements them. This "full-stack" approach on the mobile device, encompassing behavioral analysis during dApp interaction, pre-signing validation, and leveraging hardware TEEs, makes SentrySol a critical, multi-layered defense. It effectively provides the missing piece for truly secure Web3 mobile interactions, creating a more robust and resilient ecosystem.

Table 4: SentrySol's Competitive Differentiation Matrix

Security Solution Category	Primary Focus/Layer	Key Strength	Key Limitation (addressed by SentrySol)	SentrySol's Complementary/ Unique Role
General Antivirus (e.g., Kaspersky)	General malware detection, OS-level protection	Broad protection against known threats	Not specialized for Web3 behaviors/transactions	Specialized for Web3-specific behavioral threats
Device Security Platforms (e.g., Samsung Knox)	Hardware-level OS security, secure boot, data isolation	OS hardening, secure element for credentials	Focuses on OS, lacks intelligent dApp behavioral analysis	Provides crucial application-layer behavioral defense for Web3 interactions
Cloud-Based Web3 Security (e.g., Fireblocks, Zengo, Certik)	Centralized transaction monitoring, key management (MPC), code audits	Scalable analysis, multi-party key security, pre-deployment checks	Reliance on centralized servers (privacy/latency), often reactive, limited on-device context	Fully on-device operation ensures unparalleled privacy, real-time continuous protection
Hardware Wallets (e.g., Ledger, Solana SeedVault)	Secure final signing process, private key custody	Offline key storage, tamper-proof signing	No pre-signing intelligence, cannot prevent user deception by malicious frontends	Provides intelligent, real-time behavioral analysis *before* transaction reaches signing stage (pre-signing intelligence)

Auditing Firms (e.g., 8kSec, Certik)	Pre-deployment static analysis of smart contracts/code	Identification of vulnerabilities before deployment	Static analysis, no runtime protection against live, evolving threats or user-centric exploits	Offers dynamic, real-time runtime protection against live, evolving threats and user-centric exploits

7. Roadmap (Conceptual)

SentrySol's strategic roadmap outlines a phased approach to market entry and expansion, designed to establish a strong foothold in the Web3 mobile security landscape and continuously adapt to its evolving demands.

- **Q3 2025:** The immediate focus is on the **launch of SentrySol for Solana Mobile Seeker (initial version)**. This provides a strategic beachhead, leveraging the Seeker's significant market interest, evidenced by over 140,000 pre-orders across 57 countries before its 2025 release.[58] The Seeker's built-in SeedVault TEE offers an ideal environment for SentrySol's deep hardware and on-device AI integration.[51] This initial focus functions as a "lighthouse" project, demonstrating the technology's capabilities and building credibility in a controlled, high-profile environment. Simultaneously, **pilot programs with selected dApps and wallet providers** will commence to establish early partnerships and gather crucial real-world usage data. This data will be vital for **gathering initial behavioral data for AI model refinement**, a continuous process that improves the accuracy and adaptability of the on-device AI models, particularly for Federated Learning, which enables collaborative learning without compromising individual user privacy.[24]
- **Q4 2025:** SentrySol plans to **introduce its SDK for broader Web3 wallet integration (Android)**. This expansion aims to reach the rapidly growing crypto wallet market, particularly hot wallets, which constituted 56% of the market in 2024 and are instrumental in driving mass adoption of Web3.[60] The AI model capabilities will be continuously expanded for enhanced detection of new attack vectors. This commitment to continuous learning and adaptation is essential for addressing "model drift" and the constantly evolving nature of cyber threats, ensuring the long-term effectiveness of the solution.[29] Community feedback and feature iteration will also be prioritized to ensure product-market fit and user satisfaction. This phased approach demonstrates a well-thought-out growth

strategy aimed at systematically capturing significant market share across the rapidly expanding Web3 mobile landscape.

- **2026:** The long-term vision includes **expansion to other major Web3 mobile ecosystems (e.g., EVM-compatible chains on mobile)**, capitalizing on the broader Web3 market growth projected to reach $81.5 billion by 2030, and the increasing diversity of dApps.[62] SentrySol will also **explore white-label partnerships with Mobile OEMs**. This aims for deeper integration and pre-installation of SentrySol as a foundational security layer on Web3-native smartphones, tapping into the emerging trend of blockchain-enabled phones with built-in security features.[66] Further enhancements to **federated learning capabilities for faster threat adaptation** will ensure long-term resilience against zero-day and evolving social engineering attacks. Finally, the development of **advanced reporting and forensic tools for integrated partners** will extend SentrySol's value proposition beyond immediate prevention to include post-incident analysis and broader ecosystem security intelligence, such as identifying patterns of coordinated attacks and tracing malicious activities.[39] This commitment to continuous learning and adaptation ensures SentrySol's long-term relevance and effectiveness in a dynamic threat landscape, providing confidence to future partners and users that the solution will remain robust against emerging threats.

8. Conclusion

The future of Web3 is undeniably mobile, and the security of its users must be a paramount consideration, not an afterthought. The analysis presented in this whitepaper underscores that the rapid growth of the Web3 mobile ecosystem is accompanied by escalating and increasingly sophisticated security threats, particularly human-centric attacks like phishing and blind signing, which have resulted in billions of dollars in losses and significantly eroded user trust.[1] This erosion of trust directly impedes the mass adoption of decentralized technologies, positioning security as a fundamental enabler for Web3's full potential.

SentrySol provides the essential, intelligent, and privacy-preserving security layer needed to unlock the full potential of decentralized applications on mobile devices. By integrating cutting-edge AI directly on the device—leveraging TinyML for efficiency, Transformers for sequential behavioral analysis, and Graph Neural Networks for complex dApp interaction mapping—SentrySol establishes a dynamic "behavioral fingerprint of intent." This multi-modal AI approach allows for the detection of subtle, multi-faceted anomalies that single-model solutions would miss, representing a proactive paradigm shift from reactive security.

Furthermore, SentrySol's deep integration with hardware-level protection, specifically Trusted Execution Environments like Solana Mobile's SeedVault, is critical. This extends beyond mere key protection to securing the core AI logic and its parameters within a tamper-proof environment, establishing a "trusted AI" paradigm on the device itself. This level of hardware-backed AI integrity is crucial for user confidence in autonomous security decisions. The commitment to on-device processing and privacy-preserving Federated Learning ensures superior data sovereignty and continuous adaptation to new threats without compromising user data, aligning perfectly with the core tenets of Web3.

SentrySol's value proposition extends beyond immediate threat mitigation; it is positioned as a foundational enabler for the widespread adoption and success of the entire Web3 mobile ecosystem by building the necessary trust and confidence. By offering a comprehensive, multi-layered defense that complements existing security solutions and fills critical gaps, SentrySol empowers users with confidence, fostering a secure and trustworthy Web3 ecosystem.

We invite partners, developers, and users to join SentrySol in building a safer digital future.

9. Contact & Resources

- Website : sentrysol.xyz
- Email : info@sentrysol.xyz

Works cited

1. *Web3 Attacks Result in $2.3Bn in Cryptocurrency Losses - Infosecurity Magazine, accessed July 8, 2025, https://www.infosecurity-magazine.com/news/web3-attacks-cryptocurrency-losses/*
2. *The Future of Human Rights on web3 | Polaris Project, accessed July 8, 2025, https://polarisproject.org/wp-content/uploads/2022/06/The-Future-of-Human-Rights-on-web3.pdf*
3. *Cybersecurity Attacks and Detection Methods in Web 3.0 Technology: A Review - MDPI, accessed July 8, 2025, https://www.mdpi.com/1424-8220/25/2/342*
4. *What Is Decentralized Identity? A Comprehensive Guide, accessed July 8, 2025, https://www.identity.com/decentralized-identity/*
5. *Cybersecurity Implications for Web3 Trends | by Anonymous Security - Medium, accessed July 8, 2025, https://medium.com/@anonsecurity/cybersecurity-in-the-web3-age-trends-challenges-6e3344f9f910*
6. *Web3 Operational Security: Lessons from the Bybit $1.4B Wallet Safe Hack, accessed July 8, 2025, https://dev.to/nomzykush/web3-operational-security-lessons-from-the-bybit-14b-wallet-safe-hack-363i*
7. *Web3 Security Incidents Result in Significant Losses in 2025 - Binance, accessed July 8, 2025, https://www.binance.com/en/square/post/06-30-2025-web3-security-incidents-result-in-significant-losses-i*

n-2025-26317640746434

8. FreeDrain Phishing Scam Drains Crypto Hobbyists' Wallets - Infosecurity Magazine, accessed July 8, 2025, https://www.infosecurity-magazine.com/news/freedrain-phishing-scam-crypto/
9. After Bybit's $1.5B Blind Signing Fiasco, Human Wallet Steps Up with a Radical Security Fix, accessed July 8, 2025, https://hackernoon.com/after-bybits-$15b-blind-signing-fiasco-human-wallet-steps-up-with-a-radical-security-fix
10. Blind Signing Protection For EVM Chains: Bringing Transaction Transparency to Cold Wallet Security - Liminal Custody, accessed July 8, 2025, https://www.liminalcustody.com/blog/blind-signing-protection-for-evm-chains-bringing-transaction-transparency-to-cold-wallet-security/
11. 7 Smart Contract Vulnerabilities & How to Prevent Them [2025] - PixelPlex, accessed July 8, 2025, https://pixelplex.io/blog/smart-contract-vulnerabilities/
12. Top 6 Smart Contract Vulnerabilities - InApp, accessed July 8, 2025, https://inapp.com/blog/top-6-smart-contract-vulnerabilities/
13. Avoid Crypto Scams and Keep Your Money Safe in Web3: Part 1, accessed July 8, 2025, https://www.cyfrin.io/blog/how-to-avoid-crypto-scams-and-not-lose-money-in-web3-part-1
14. Solana Hacks, Bugs, and Security Exploits: A Complete History - Helius, accessed July 8, 2025, https://www.helius.dev/blog/solana-hacks
15. HISTORY OF SOLANA SECURITY INCIDENTS: HACKS, HALTS AND HARD LESSONS., accessed July 8, 2025, https://medium.com/@i2032084/history-of-solana-security-incidents-hacks-halts-and-hard-lessons-13d3052297c9
16. The Road to Web3 Mass Adoption: Paved with Security, Not Just UX and Gas | The Block, accessed July 8, 2025, https://www.theblock.co/post/359828/the-road-to-web3-mass-adoption-paved-with-security-not-just-ux-and-gas
17. PhishSense-1B: A Technical Perspective on an AI-Powered Phishing Detection Model, accessed July 8, 2025, https://arxiv.org/html/2503.10944v1
18. AI Phishing Detection - E & E Tech, accessed July 8, 2025, https://poweronpro.com/services/ai-phishing-detection/
19. What Is Behavioral Biometrics? - BioCatch, accessed July 8, 2025, https://www.biocatch.com/blog/what-is-behavioral-biometrics
20. Behavioral Biometrics for Mobile App Security: Complete Guide - Marketsy.ai, accessed July 8, 2025, https://marketsy.ai/blog/behavioral-biometrics-for-mobile-app-security-complete-guide
21. On-Device AI Models: Advancing Privacy-First Machine Learning for Mobile Applications, accessed July 8, 2025, https://www.researchgate.net/publication/387706168_On-Device_AI_Models_Advancing_Privacy-First_Machine_Learning_for_Mobile_Applications
22. Why TinyML is the Next Big Thing in AI and IoT - Ascentt, accessed July 8, 2025, https://www.ascentt.com/why-tinyml-is-the-next-big-thing-in-ai-and-iot/
23. TinyML: Edge AI for Resource-Constrained Devices | by Pete Weishaupt | Jun, 2025, accessed July 8, 2025, https://peteweishaupt.medium.com/tinyml-edge-ai-for-resource-constrained-devices-437630446619
24. Federated learning for privacy-preserving data analytics in mobile applications, accessed July 8, 2025, https://www.researchgate.net/publication/391323029_Federated_learning_for_privacy-preserving_data_analytics_in_mobile_applications
25. On-Device Learning TinyML for Anomaly Detection Based on Extreme Values Theory, accessed July 8, 2025, https://www.researchgate.net/publication/373944123_On-Device_Learning_TinyML_for_Anomaly_Detection_Based_on_Extreme_Values_Theory
26. Tiny ML optimization - Cyient, accessed July 8, 2025, https://www.cyient.com/whitepaper/tiny-ml-optimization
27. Robust Watermarking of Tiny Neural Networks by Fine-Tuning and Post-Training Approaches - MDPI, accessed July 8, 2025, https://www.mdpi.com/2073-8994/17/7/1094
28. Tiny Machine Learning and On-Device Inference: A Survey of Applications, Challenges, and Future Directions - PubMed Central, accessed July 8, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC12115890/
29. Real-Time Anomaly Detection Using Transformer-Based Architectures in Cloud Traffic, accessed July 8, 2025, https://www.researchgate.net/publication/391768629_Real-Time_Anomaly_Detection_Using_Transformer-Based_Architectures_in_Cloud_Traffic
30. Research and application of Transformer based anomaly detection model - arXiv, accessed July 8, 2025, https://arxiv.org/pdf/2402.08975
31. Enhancing Insider Threat Detection Using User-Based Sequencing and Transformer Encoders - arXiv, accessed July 8, 2025, https://arxiv.org/html/2506.23446v1

32. *(PDF) A Transformer-based GAN for Anomaly Detection - ResearchGate, accessed July 8, 2025, https://www.researchgate.net/publication/362028308_A_Transformer-based_GAN_for_Anomaly_Detection*
33. *Towards Enhanced IoT Security: Advanced Anomaly Detection using Transformer Models, accessed July 8, 2025, https://ai4cyber-kdd.com/KDD-AISec_files/Submission_7_final.pdf*
34. *LogLLaMA: Transformer-based log anomaly detection with LLaMA - arXiv, accessed July 8, 2025, https://arxiv.org/html/2503.14849v1*
35. *Real-Time Anomaly Detection Using Transformer-Based Architectures in Cloud Traffic, accessed July 8, 2025, https://www.researchgate.net/publication/391768196_Real-Time_Anomaly_Detection_Using_Transformer-Based_Architectures_in_Cloud_Traffic*
36. *Graph Neural Networks (GNNs) - Comprehensive Guide - viso.ai, accessed July 8, 2025, https://viso.ai/deep-learning/graph-neural-networks/*
37. *Leveraging Graph Neural Networks for Enhanced Security and ..., accessed July 8, 2025, https://www.splunk.com/en_us/blog/artificial-intelligence/splunk-graph-neural-networks-security-observability.html*
38. *Review of blockchain application with Graph Neural Networks, Graph Convolutional Networks and Convolutional Neural Networks - arXiv, accessed July 8, 2025, https://arxiv.org/html/2410.00875v1*
39. *Detecting Anomalies in Blockchain Transactions Using Spatial-Temporal Graph Neural Networks - ResearchGate, accessed July 8, 2025, https://www.researchgate.net/publication/390130937_Detecting_Anomalies_in_Blockchain_Transactions_Using_Spatial-Temporal_Graph_Neural_Networks*
40. *Supercharging Fraud Detection in Financial Services with Graph Neural Networks (Updated) | NVIDIA Technical Blog, accessed July 8, 2025, https://developer.nvidia.com/blog/supercharging-fraud-detection-in-financial-services-with-graph-neural-networks/*
41. *AI-Powered Fraud Detection in Digital Payment Systems: Leveraging Machine Learning for Real-Time Risk Assessment - Preprints.org, accessed July 8, 2025, https://www.preprints.org/manuscript/202502.0278/v1*
42. *AI Fraud Detection in Crypto Transactions: How It Works & Why It Matters - Sunrise Technologies, accessed July 8, 2025, https://www.sunrisetechs.com/ai-fraud-detection-crypto-transactions/*
43. *Motion recognition + anomaly detection | Edge Impulse ..., accessed July 8, 2025, https://docs.edgeimpulse.com/docs/tutorials/end-to-end-tutorials/time-series/continuous-motion-recognition*
44. *Review on Deep Learning Approaches for Anomaly Event Detection in Video Surveillance, accessed July 8, 2025, https://www.mdpi.com/2079-9292/12/1/29*
45. *(PDF) Future Trends in AI-Driven Behavioral Authentication: What's Next for Cybersecurity?, accessed July 8, 2025, https://www.researchgate.net/publication/390528947_Future_Trends_in_AI-Driven_Behavioral_Authentication_What's_Next_for_Cybersecurity*
46. *10 App Security Best Practices for AI Threats - Rocket Farm Studios, accessed July 8, 2025, https://www.rocketfarmstudios.com/blog/10-app-security-best-practices-for-ai-threats/*
47. *OIL-AD: An Anomaly Detection Framework for Sequential Decision Sequences - arXiv, accessed July 8, 2025, https://arxiv.org/pdf/2402.04567*
48. *Introduction to Trusted Execution Environments | GlobalPlatform, accessed July 8, 2025, https://globalplatform.org/wp-content/uploads/2018/05/Introduction-to-Trusted-Execution-Environment-15May2018.pdf*
49. *Trusted execution environment - Wikipedia, accessed July 8, 2025, https://en.wikipedia.org/wiki/Trusted_execution_environment*
50. *Seed Vault | Solana Mobile Docs, accessed July 8, 2025, https://docs.solanamobile.com/developers/seed-vault*
51. *What Is Solana Mobile Phone? Everything About Solana Seeker Phone Features, Benefits And Price | MEXC Blog, accessed July 8, 2025, https://blog.mexc.com/what-is-solana-mobile-phone/*
52. *Can a TEE be used to secure machine learning models and data in a high-performance computing system?, accessed July 8, 2025, https://massedcompute.com/faq-answers/?question=Can+a+TEE+be+used+to+secure+machine+learning+models+and+data+in+a+high-performance+computing+system%3F*
53. *Integrating Large Language Models in Trusted Execution Environments with SuperMQ and Ollama | by Rodney Osodo | Ultraviolet Blog | Medium, accessed July 8, 2025, https://medium.com/ultraviolet-blog/integrating-large-language-models-in-trusted-execution-environments-with-supermq-and-ollama-b70307d327ad*
54. *Trusted Execution Environment (TEE) - Learn Microsoft, accessed July 8, 2025, https://learn.microsoft.com/en-us/azure/confidential-computing/trusted-execution-environment*
55. *Trusted Machine Learning Models Unlock Private Inference for Problems Currently Infeasible with*

Cryptography - arXiv, accessed July 8, 2025, https://arxiv.org/html/2501.08970v1

56. Privacy-Preserving Anomaly Detection via Federated Learning in Multi-Tenant Clouds, accessed July 8, 2025, https://www.researchgate.net/publication/391449933_Privacy-Preserving_Anomaly_Detection_via_Federated_Learning_in_Multi-Tenant_Clouds
57. Solana's New Crypto Phone Seeker: Features, Specs and Shipping Dates | CCN.com, accessed July 8, 2025, https://www.ccn.com/news/technology/solanas-new-crypto-phone-seeker-features-specs/
58. Demand for Solana's unreleased phone is so hot orders have already hit $70m - DL News, accessed July 8, 2025, https://www.dlnews.com/articles/web3/solana-mobile-crypto-phone-hits-usd-70-million-in-preorders/
59. Solana Reveals Seeker, Now with 140,000+ Units Sold in Presale - NFT Plazas, accessed July 8, 2025, https://nftplazas.com/solana-seeker/
60. Crypto Wallet Market Size And Share | Industry Report, 2033 - Grand View Research, accessed July 8, 2025, https://www.grandviewresearch.com/industry-analysis/crypto-wallet-market-report
61. Web3 Wallet Market Research Report 2033, accessed July 8, 2025, https://growthmarketreports.com/report/web3-wallet-market
62. Market Analysis of 10 Most popular dApps - Pontem Network, accessed July 8, 2025, https://pontem.network/posts/market-analysis-of-10-most-popular-dapps
63. Dapp Industry Report – 2024 Overview - DappRadar, accessed July 8, 2025, https://dappradar.com/blog/dapp-industry-report-2024-overview
64. Safeguard your DApp with a security audit - ShellBoxes, accessed July 8, 2025, https://shellboxes.com/blog/protect-your-dapp-with-a-security-audit/
65. Regulatory Challenges in DApp Development - Key Questions Every Blockchain Developer Must Consider - MoldStud, accessed July 8, 2025, https://moldstud.com/articles/p-regulatory-challenges-in-dapp-development-key-questions-every-blockchain-developer-must-consider
66. Top 7 Web3 Phones for Secure Crypto Asset Management - Vertu, accessed July 8, 2025, https://vertu.com/lifestyle/top-7-web3-phone-models-2025-secure-crypto-asset-management/
67. IMPulse K1 Encrypted Smartphone - CryptoDATA, accessed July 8, 2025, https://en.cryptodata.com/impulse
68. AlphaPoint | White Label Cryptocurrency Exchange Software, accessed July 8, 2025, https://alphapoint.com/
69. White Label & Branded Access Solutions - Tapkey, accessed July 8, 2025, https://tapkey.io/en/tapkey-white-label-solutions/
70. AI-Enhanced White Label Softphones for Smart Communication Systems - Fonimo, accessed July 8, 2025, https://fonimo.app/blog/ai-enhanced-white-label-softphones-for-smart-communication-systems/
71. White Label - Jervis Systems, accessed July 8, 2025, https://www.jervis.systems/white-label
72. AI-Powered Anomaly Detection with Blockchain for Real-Time Security and Reliability in Autonomous Vehicles - arXiv, accessed July 8, 2025, https://arxiv.org/html/2505.06632v1
73. Combat Cyber Threats With AI-Driven Threat Intelligence - Cyble, accessed July 8, 2025, https://cyble.com/knowledge-hub/combat-cyber-threats-ai-driven-threat-intelligence/
74. AI in Web3: Unlocking Intelligence and Scale in Decentralized App Ecosystems - Calibraint, accessed July 8, 2025, https://www.calibraint.com/blog/ai-in-web3
75. Web 3.0 Market Size, Share | Industry Forecast by 2030 - Emergen Research, accessed July 8, 2025, https://www.emergenresearch.com/industry-report/web-3-market
76. Kaspersky Cyber Security Solutions for Home and Business | Kaspersky, accessed July 8, 2025, https://usa.kaspersky.com/
77. Samsung Introduces Future-Ready Mobile Security for Personalized AI Experiences, accessed July 8, 2025, https://news.samsung.com/global/samsung-introduces-future-ready-mobile-security-for-personalized-ai-experiences
78. Samsung Knox | Secure mobile platform and solutions, accessed July 8, 2025, https://www.samsungknox.com/en
79. Main Capabilities - Embedded Wallet Overview - Fireblocks, accessed July 8, 2025, https://ncw-developers.fireblocks.com/docs/main-capabilities
80. What Is Fireblocks? - Gate.com, accessed July 8, 2025, https://www.gate.com/learn/articles/what-is-fireblocks/7863
81. Zengo Pro: Your Complete Guide to the best crypto wallet protection, accessed July 8, 2025, http://help.zengo.com/en/articles/8105588-zengo-pro-your-complete-guide-to-the-best-crypto-wallet-protection
82. Theft Protection - The Most Secure Crypto Wallet - Zengo, accessed July 8, 2025, https://zengo.com/pro-theft-protection/
83. Elevate Your Web3 Journey - CertiK, accessed July 8, 2025, https://www.certik.com/?ref=vintages
84. Ledger Crypto Wallet - Security for DeFi & Web3, accessed July 8, 2025, https://www.ledger.com/SentrySol's technological framework rests upon three foundational pillars: AI-Native and On-Device Processing, Privacy-Preserving Federated Learning, and Hardware-Level Security. These components collectively deliver

a robust, efficient, and user-centric security solution for the Web3 mobile ecosystem.