



GuardApp Corporation

Know Before You Swap

GUARD CORPORATION

A Canadian-Based company



The Solana Transaction Intelligence Platform

Technical White Paper v2.0 · August 2026

guardapp.ca · [X / Twitter](#) · [Discord](#) · [Telegram](#)

[YouTube](#) · [TikTok](#) · [Instagram](#) · [Facebook](#)



GuardApp Corporation

Know Before You Swap

Table of Contents

1. Executive Summary
2. The Problem: Structural Value Extraction on Solana
3. The GUARD Solution: Simulate Before You Execute
4. Technical Architecture: The Simulation Engine
5. The Eleven-Layer Protection Model
6. Counter-Trade Intelligence (CTI)
7. The GUARD Token: Utility-Driven Economic Design
8. Tokenomics: Supply, Distribution & Vesting
9. Revenue Model & Economic Sustainability
10. Competitive Landscape & Market Opportunity
11. Roadmap
12. Security Architecture & User Protection
13. Team
14. Risk Factors & Disclaimer
15. Conclusion



GuardApp Corporation

Know Before You Swap

1. Executive Summary

"Every dollar lost to a failed transaction, every cent bled by excessive slippage, every trade stolen by a sandwich attack, every wallet drained by a honeypot token, none of it needed to happen."

GUARD is a **read-only Solana transaction protection layer** that intercepts decentralized exchange (DEX) swap transactions before they reach the Solana blockchain. Using a production-grade simulation engine backed by eleven specialized protection modules, GUARD tests every trade across a five-level slippage ladder, 0.5%, 1%, 2%, 3%, and 5%, scans token contracts for nine risk flags, detects MEV sandwich attacks from 20+ known bot addresses, compares execution routes across Jupiter, Raydium, and Orca simultaneously, profiles every counterparty wallet for eight behavioral risk patterns, and either allows the trade at the best possible execution or blocks it entirely before a single unit of value is spent.

The economics are immediate and verifiable. A trader executing 100 swaps per month who saves \$15 per trade through optimized slippage and blocked failed transactions saves approximately **\$1,500 per month**: against a subscription cost of \$8.99 to \$16.99. The platform displays these savings live on a per-trade dashboard, verified against the user's own on-chain wallet history. The ROI is not theoretical. It is calculated, displayed, and proven.

GUARD is built on a 31-file simulation engine deployed on Vercel's serverless infrastructure, backed by a PostgreSQL database accessed through Drizzle ORM, with a multi-provider RPC pool providing redundant Solana connectivity through Helius, Chainstack, Triton, QuickNode, Alchemy, and public fallback nodes. The frontend is a React 19 SPA powered by tRPC for end-to-end type safety, Tailwind CSS v4, and shadcn/ui components.

The GUARD token is an SPL token on Solana with fixed 1 billion supply. It unlocks discounted subscription tiers, powers the loyalty rewards system, and serves as the utility key to the entire GUARD ecosystem. Holding \$50 worth of GUARD unlocks the Pro tier. Holding \$100 worth of GUARD unlocks the VIP tier with full Counter-Trade Intelligence and counterparty profiling. The token presale launches August 20, 2026 on PinkSale.



GuardApp Corporation

Know Before You Swap

This white paper is a technical reference. It describes the problem, the solution, the architecture, the protection layers, the tokenomics, and the roadmap. It is not an invitation to invest. It is an explanation of why GUARD exists, how it works at the protocol level, and what it means for the future of safe trading on Solana.

2. The Problem: Structural Value Extraction on Solana

2.1 The Solana Paradox

Solana is one of the most technically impressive blockchains ever built. Four hundred millisecond block times. Sub-cent transaction fees. A thriving ecosystem of decentralized exchanges processing billions in daily volume. By every standard metric of blockchain performance, Solana delivers.

But raw throughput does not equal safe execution. The same architectural properties that make Solana fast, its parallel transaction processing, its lack of a traditional mempool, its Turbine block propagation, also create unique attack surfaces. And the ecosystem's permissionless token creation, while democratizing access, has also democratized fraud. The result is a cascade of preventable value extraction that costs traders an estimated **\$20–25 billion annually** across hacks, scams, rug pulls, MEV extraction, and transaction failure waste.

Below, we decompose each vector of loss and map it to the specific protection layer GUARD deploys against it.

2.2 Failed Transactions: Paying for Nothing

Root Cause: Solana's transaction processing model charges compute units regardless of outcome. When a DEX swap fails, because price moved past the slippage threshold between submission and confirmation, a liquidity pool was drained by a competing transaction, or the network experienced a congestion spike, the transaction still consumes compute budget and the user still pays the priority fee.

Quantified Impact: A single failed swap costs approximately \$0.005 to \$0.02 in priority fees. An active trader executing 200 swaps monthly at a 20% failure rate incurs \$15–\$40 in wasted



GuardApp Corporation

Know Before You Swap

costs on failed transactions alone, before any slippage loss is factored in. For high-frequency traders and bot operators, the cumulative waste reaches hundreds of dollars monthly.

Structural Flaw: Traders submit transactions **blindly**. They discover failure only after the blockchain has processed, and billed, their attempt. There is no pre-flight validation, no safety net, no simulation layer between intent and execution.

GUARD Defense → Layer 1 (Pre-Execution Simulation) + Layer 10 (RPC Redundancy & Failover): GUARD intercepts the transaction before broadcast, simulates it against the current blockchain state using Solana's simulateTransaction RPC, and only allows broadcast if the simulation confirms successful execution. Failed simulations block the transaction. No gas is ever paid for a doomed trade.

2.3 Excessive Slippage: The Insurance Tax

Root Cause: To compensate for Solana's speed-induced price volatility and reduce failure risk, traders set slippage tolerances higher than necessary. A trader who could execute at 1% slippage sets 5% "just to be safe." The trade succeeds, but the trader pays 4% more than required. This excess is invisible: the trade shows as "successful," and most wallets provide no feedback on how much value was lost to unnecessarily wide tolerances.

Quantified Impact: On a \$1,000 trade, 4% excess slippage costs \$40. On a \$10,000 trade, \$400. Over hundreds of trades, excessive slippage quietly drains portfolios by thousands of dollars monthly. The loss is cumulative, invisible, and entirely preventable.

Structural Flaw: No existing Solana tool answers the question: *"What is the minimum slippage at which this trade will succeed right now?"* Traders guess. They guess high. They lose.

GUARD Defense → Layer 7 (Slippage Ladder Intelligence): GUARD tests the trade at five discrete slippage levels, 0.5%, 1%, 2%, 3%, 5%, in parallel. It identifies the lowest passing level and recommends execution at that exact tolerance. The difference between the trader's typical 5% setting and GUARD's optimized 1–2% recommendation is pure savings, calculated and displayed with each trade.



GuardApp Corporation

Know Before You Swap

2.4 MEV & Sandwich Attacks: Invisible Value Extraction

Root Cause: Maximal Extractable Value (MEV) bots monitor pending transaction flows. When they detect a large swap, they execute a sandwich: front-run (buy the same asset to push price up), let the victim's trade execute at the inflated price, then back-run (sell immediately, capturing the spread). The victim's trade "succeeds", but at a systematically worse price than fair market value.

Quantified Impact: MEV extraction on Solana is estimated in the hundreds of millions to low billions annually, distributed across millions of micro-extractions. Individual traders rarely notice, the trade shows as completed, and wallets don't flag MEV-impacted prices. But the aggregate drain is massive.

Structural Flaw: Solana's scheduler model creates unique MEV vectors. Sandwich bots are identifiable by their transaction patterns and known wallet addresses, but no consumer tool currently screens for them pre-trade.

GUARD Defense → Layer 4 (MEV & Sandwich Protection): GUARD maintains a registry of 20+ known MEV bot addresses, integrates with Jito bundle data for real-time mempool monitoring, applies pattern recognition to detect front-run/back-run sequences, and scores each trade's MEV risk on a five-tier scale. When MEV risk is detected, GUARD can recommend higher slippage to absorb the attack, route through an alternative DEX where the bot is not active, or warn the user with a risk score before commitment.

2.5 Scam Tokens, Honeypots & Rug Pulls

Root Cause: Solana's permissionless token creation allows anyone to deploy a token with malicious contract logic. Common attack patterns include:

- **Honeypots:** A honeypot program allows buys but blocks or severely restricts sells through modified transfer hook programs. A honeypot traps buyer funds permanently.
- **Hidden Transfer Taxes:** The token program imposes fees far higher than advertised, sometimes 50% or more, silently applied at the protocol level during every transfer.



GuardApp Corporation

Know Before You Swap

- **Active Mint Authority:** The deployer retains the ability to mint unlimited new tokens, diluting existing holders to zero.
- **Freeze Authority:** The deployer can freeze individual token accounts, preventing the holder from transferring or selling.
- **Blacklist Functions:** Specific wallet addresses can be programmatically blocked from transferring or selling.
- **Proxy/Upgradeable Contracts:** The token's program can be replaced with new logic after deployment, changing its behavior retroactively.
- **Unverified Source Code:** The deployed bytecode does not match any publicly available source, making manual audit impossible.
- **Rug Pull History:** The deployer address or contract is linked to previous rug pulls through on-chain forensics.

Quantified Impact: In 2025, an estimated \$1.8–2.8 billion was drained in rug pulls alone. 62% of newly launched meme coins exhibited scam characteristics. The FBI's Internet Crime Complaint Center reported \$11.4 billion in crypto fraud, up 22% year-over-year. Chainalysis documented \$14–17 billion received by scammers on-chain in 2025.

Structural Flaw: No Solana DEX or aggregator screens tokens for contract-level risk before a trade executes. Manual research, checking explorers, reading contract code, searching social media, takes time, requires expertise, and is error-prone. Most traders skip it entirely.

GUARD Defense → Layer 2 (Token Contract Scanning) + Layer 8 Extension (Honeypot Detection): GUARD integrates three data sources: RugCheck.xyz community-vetted risk reports, Birdeye token metadata and holder analysis, and direct on-chain heuristic inspection. It checks for nine risk flags before any simulation runs. The Honeypot Detector goes further, it simulates both a buy and a sell transaction to verify that tokens can actually be sold after purchase. Risk is tiered: Safe (green), Suspicious (yellow), High Risk (orange), Critical/Honeypot (red). Critical-risk tokens are blocked outright with a detailed explanation.



GuardApp Corporation

Know Before You Swap

2.6 Suboptimal DEX Routing

Root Cause: Most Solana traders use a single DEX, typically Jupiter, Raydium, or Orca, without comparing execution quality across venues. Different DEXes maintain different liquidity pools with different depths, fee structures, and price curves. A trade that would experience 3% price impact on Raydium might execute at 1% on Jupiter's optimal route through multiple pools.

Quantified Impact: Cross-DEX price dispersion on Solana typically ranges from 0.5% to 3% for major pairs and can exceed 5% for low-liquidity tokens. A trader routing \$5,000 through a suboptimal venue loses \$25–\$150 per trade, thousands per month.

GUARD Defense → Layer 3 (Cross-DEX Price Comparison): GUARD queries Jupiter's quote API for multiple route options, then simulates execution across Jupiter, Raydium, and Orca simultaneously. It selects the route that delivers the maximum output tokens at the minimum required slippage, with per-route price impact and fee comparison.

2.7 Liquidity Risk & Whale Manipulation

Root Cause: Trading on low-liquidity pools creates extreme price impact. A \$5,000 swap on a pool with \$12,000 total liquidity can move the price by 20%+ before the trade completes. Additionally, large holders (whales) can dump positions mid-execution, crashing the price between the moment a trader submits and the moment the blockchain confirms.

GUARD Defense → Layer 6 (Liquidity Depth Analysis) + Layer 8 (Whale Watch Alerts): The Liquidity Analyzer checks actual pool depth before simulation, calculates expected price impact based on the constant product formula or concentrated liquidity math, and flags trades where the trade size exceeds a safe threshold relative to available liquidity. The Whale Watcher tracks wallets holding more than 1% of a token's supply, monitoring for accumulation and dumping patterns that could affect trade execution.

2.8 The Unified Problem Statement

The common thread across all seven loss vectors is **information asymmetry at the point of execution**. Traders submit transactions without knowing:

**GuardApp Corporation**

Know Before You Swap

1. Whether the transaction will succeed (failed transactions)
2. What the minimum viable slippage is (excessive slippage)
3. Whether MEV bots are targeting their pool (sandwich attacks)
4. Whether the token contract is malicious (scam tokens)
5. Whether a better price exists on another venue (suboptimal routing)
6. Whether the pool has sufficient depth (liquidity risk)
7. Whether whales are about to dump (whale manipulation)
8. Who is on the other side of the trade (counterparty risk)

GUARD eliminates this information asymmetry. It answers all eight questions before a single transaction reaches the blockchain.

2.9 Problem → Defense Summary Matrix

#	Loss Vector	Annual Impact	Who It Affects	Root Cause	GUARD Defense Layer
1	Failed Transactions	\$15–\$40/month per active trader	Every DEX user	No pre-flight validation; pay gas regardless of outcome	Layer 1: Pre-Execution Simulation
2	Excessive Slippage	1–5% of every trade, \$100s/month	Traders using manual slippage	No tool tells you the minimum viable slippage	Layer 7: Slippage Ladder Intelligence
3	MEV Sandwich Attacks	Hundreds of millions/year ecosystem-wide	Mid-to-large swap traders	Bots front-run visible pending transactions	Layer 4: MEV & Sandwich Protection



4	Scam Tokens & Honey pots	\$1.8–2.8 billion in 2025	Memecoin/altcoin traders	Permissionless token creation; no pre-trade screening	Layer 2: Token Contract Scanning + Honey pot Detector
5	Suboptimal DEX Routing	0.5–5% per trade	Single-DEX users	No cross-venue comparison before execution	Layer 3: Cross-DEX Route Optimization
6	Liquidity Risk	3–20%+ price impact on small pools	Low-cap token traders	No pre-trade depth vs. size ratio check	Layer 6: Liquidity Depth Analysis
7	Whale Manipulation	Position-crashing mid-execution	Holders of concentrated-supply tokens	No large-holder movement monitoring	Layer 8: Whale Watch Alerts
8	Counterparty Risk	Unknown; historically unmeasured	All traders	Zero visibility into who is on the other side	Layer 8 ext: Counter-Trade Intelligence (VIP)

Each row above maps a proven, recurring loss vector directly to a specific, engineered protection layer within the GUARD platform. No other Solana tool addresses more than two of these vectors simultaneously.

3. The GUARD Solution: Simulate Before You Execute

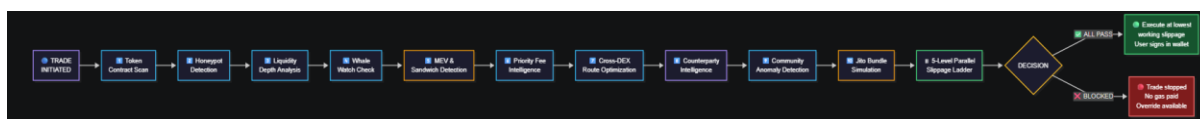
3.1 The Core Innovation

GUARD changes the execution model from **submit-and-pray** to **simulate-then-execute**. It sits as a read-only layer between the user's wallet and the Solana blockchain, analyzing, simulating, and validating every trade before it ever touches the network.

The architecture is fundamentally non-custodial. GUARD connects to wallets in read-only mode using the Solana wallet adapter standard. It can view public keys and token balances. It can simulate transactions against the current blockchain state. It can analyze token contracts and on-chain data. What it cannot do, architecturally, not just policy, is sign transactions, transfer funds, or access private keys. Transaction signing always stays in the user's wallet.

3.2 The Protection Flow

When a user initiates a trade on any supported DEX (Jupiter, Raydium, or Orca), GUARD executes the following pipeline:



Pipeline Summary: Each step is a dedicated protection subsystem. Steps 1–10 execute sequentially, detecting and flagging risks at every stage. A critical finding at any step can halt the pipeline immediately, the user is never forced through all 11 checks if a blocker is found early. Step 11 (the Slippage Ladder) always runs last, as it depends on the route and fee parameters selected by the preceding optimization steps.

3.3 The Five-Level Slippage Ladder: Technical Specification

The slippage ladder is GUARD's core execution optimization mechanism. Each level simulates the same swap transaction with a different amountOutMin parameter derived from the quoted expected output.



Level	Slippage	amountOutMin (for \$1,000 USDC → SOL at ~\$72.60/SOL)	Expected Output	Min Acceptable
1	0.5%	13.70 SOL	13.77 SOL	13.70 SOL
2	1.0%	13.64 SOL	13.77 SOL	13.64 SOL
3	2.0%	13.50 SOL	13.77 SOL	13.50 SOL
4	3.0%	13.36 SOL	13.77 SOL	13.36 SOL
5	5.0%	13.09 SOL	13.77 SOL	13.09 SOL

Algorithm: All five levels are simulated in parallel using Promise.all. The simulateTransaction RPC call is made with replaceRecentBlockhash: true and sigVerify: false to test against the current blockchain state without consuming real funds. Each simulation result is classified as pass, fail, or error.

Early Stopping: Once any level passes, remaining pending simulations are allowed to complete for data collection, but the result is immediately returned at the lowest passing level. This minimizes perceived latency, if 0.5% passes (which it does in the majority of cases), the user gets a result in under 200ms.

Failure Taxonomy: GUARD maps 24 Solana error codes into five categories:

- **Slippage errors:** SlippageToleranceExceeded, ExceededSlippage, the price moved too far
- **Account errors:** AccountNotFound, InvalidAccountData, pool state issues
- **Balance errors:** InsufficientFunds, InsufficientFundsForFee, wallet balance issues
- **Compute errors:** ComputationalBudgetExceeded, transaction complexity exceeded limits
- **Network errors:** BlockhashNotFound, TransactionExpired, RpcError, infrastructure issues



GuardApp Corporation

Know Before You Swap

Performance Targets:

Metric	Target
Single simulation (one level)	< 500ms
Full ladder (all 5 levels)	< 2.0 seconds
Early stop (0.5% passes)	< 200ms
Error rate under normal load	< 2%
Cache hit rate	40–60%

3.4 The Savings Dashboard: Verifiable Results

Every trade run through GUARD is logged to the database with: original slippage that would have been used, optimal slippage found by the ladder, SOL saved in gas fees, USD saved in slippage optimization, DEX used, token pair, and outcome (allowed/blocked). The dashboard displays:

- **Lifetime savings** in SOL and USD, calculated from cumulative per-trade deltas
- **Protection rate:** percentage of failing trades caught
- **Trade history** with filtering by DEX, pair, and outcome
- **Savings trend** over time with month-over-month comparison
- **Risk distribution:** pie chart of risk flag frequencies encountered

These figures are verifiable against the user's own wallet transaction history. Every blocked trade is a transaction that was never broadcast. Every optimized slippage is a measurable improvement over what the user would have set manually.

4. Technical Architecture: The Simulation Engine

4.1 Technology Stack

Layer	Technology	Purpose
-------	------------	---------

**GuardApp Corporation**

Know Before You Swap

Frontend	React	UI framework
	Vite	Build tool + dev server
	TypeScript	Type safety (end-to-end)
	Tailwind CSS	Utility-first styling
	shadcn/ui	Accessible UI primitives
	Framer Motion	Animation system
	Recharts	Data visualization
	Wouter	Lightweight SPA routing
	@tanstack/react-query	Server state management
	@trpc/client	Type-safe RPC client
	@solana/wallet-adapter	Read-only wallet connection
	@solana/web3.js	Solana RPC interactions
Backend	Express	HTTP server
	@trpc/server	Type-safe API framework
	Drizzle ORM	Database ORM with migrations
	PostgreSQL	Primary database
	Redis	Distributed caching
	Stripe	Payment processing
	Resend	Email delivery (OTP + notifications)
	JOSE	JWT token signing
	LRU Cache	In-memory caching
	p-queue / p-limit / p-retry	Concurrency control
	OpenTelemetry	Distributed tracing
	Pino	Structured logging
	Sentry	Error tracking
Infrastructure	Vercel	Serverless hosting
	Docker	Containerization
	GitHub Actions	CI/CD pipeline



GuardApp Corporation

Know Before You Swap

Vitest

Automated testing

The stack is selected for end-to-end type safety, serverless scalability, and Solana-native compatibility. All wallet interactions are read-only by design and enforced at the adapter level.

4.2 The Engine Architecture

The simulation engine is organized as a unified facade that orchestrates multiple specialized subsystems:

GuardEngine

└─ Infrastructure Subsystems

- └─ RPC Pool: Multi-provider load balancing
- └─ Cache Manager, Multi-tier caching
- └─ Simulation Queue, Backpressure-aware priority queuing
- └─ Metrics Manager, Latency/error/health tracking
- └─ Pool State Manager, WebSocket pool subscriptions

└─ Protection Subsystems (Pre-Simulation)

- └─ Token Scanner, RugCheck + Birdeye + on-chain heuristics
- └─ Honeypot Detector, Buy + sell simulation
- └─ Liquidity Analyzer, Pool depth + price impact
- └─ Whale Watcher, Large holder movement tracking
- └─ MEV Detector, Sandwich detection + MEV scoring
- └─ Community Anomaly, Statistical outlier + alerting

└─ Optimization Subsystems

- └─ Route Optimizer: Multi-DEX + multi-route comparison
- └─ Priority Fee Intelligence: Network congestion-aware fee analysis
- └─ Jito Simulator, Bundle-level secondary validation

└─ Intelligence Subsystems

- └─ Counterparty Intelligence: Wallet profiling + risk pattern detection



GuardApp Corporation

Know Before You Swap

- | |—— Pattern Learner, ML-driven slippage level ordering
- | |—— ML Threat Detector, ML threat detection
- | |—— Market Intelligence, Market-wide trade pattern analysis
- | |—— Smart Money Tracker, Profitable wallet following
- | |—— Flow Analyzer, Token flow analysis across wallets
- |
- |—— Feedback Subsystems
 - |—— Outcome Tracker: Post-trade verification
 - |—— Outcome Store: Outcome persistence
 - |—— Outcome Listener: Event-driven outcome processing
 - |—— Outcome Analytics: Aggregate outcome reporting

Each subsystem operates independently but passes its findings through a unified pipeline. The engine is designed so that protection, optimization, intelligence, and feedback layers can be developed, tested, and scaled independently.

4.3 RPC Connection Pool

GUARD maintains a weighted round-robin pool across multiple RPC endpoints to eliminate single-provider dependency. Providers operate across three tiers: primary, secondary, and fallback, with traffic distributed based on real-time health scoring.

Provider Strategy: Endpoints from Helius, Chainstack, Triton, QuickNode, Alchemy, and public Solana nodes are organized by priority. Each provider is continuously monitored for latency, error rate, and slot lag. When a provider degrades below acceptable thresholds, traffic is automatically redistributed to healthier endpoints.

Health Scoring: Each endpoint is evaluated on latency (both median and tail), error rate over a rolling window, and the delta between the provider's highest confirmed slot and the network-reported slot. The aggregate score determines the provider's weight in the round-robin rotation.

Circuit Breakers: Consecutive failures trigger automatic circuit breaking with graduated cooldown periods proportional to the provider's tier. After cooldown expires, a single probe



request determines whether the endpoint is healthy enough to rejoin the pool. This prevents cascading retries to failing nodes.

Blockhash Optimization: A dedicated blockhash cache pre-fetches at every slot boundary, eliminating the per-simulation blockhash RPC call and reducing simulation latency measurably.

4.4 Multi-Layer Caching Architecture

GUARD employs a tiered caching strategy to minimize redundant RPC calls:

- **Simulation Cache:** Recently simulated trades are cached to avoid re-running identical simulations within the same block window.
- **Pool State Cache:** AMM pool data is cached with volatility-aware expiration; high-volatility pairs receive shorter lifetimes to prevent stale liquidity data from driving simulations.
- **Blockhash Cache:** Pre-fetched at each slot boundary, eliminating per-simulation blockhash requests.
- **Priority Fee Cache:** Network-wide fee recommendations are cached and refreshed at sub-minute intervals.
- **Token Risk Cache:** Contract risk profiles for recently scanned tokens are retained for reuse.
- **Route Cache:** DEX route data is held stable for the duration of a block.

Cache invalidation is primarily event-driven via WebSocket subscriptions for pool state changes, with time-based fallback for other categories.

4.5 Simulation Queue & Backpressure

Under concurrent load, simulation requests enter a priority queue. VIP token holders receive a dedicated fast lane with higher throughput allocation. All other authenticated users share a standard lane.

Backpressure Strategy: As queue depth increases, the system applies graduated backpressure: first by returning rate-limit responses, then by gracefully degrading non-critical protection



GuardApp Corporation

Know Before You Swap

checks to preserve core simulation throughput. This ensures critical protection (slippage ladder, token scanning, MEV detection) remains available even during traffic spikes.

Retry Logic: Failed simulations are automatically retried through different RPC endpoints with exponential backoff, ensuring transient provider failures do not produce false negatives for users.

4.6 Metrics & Observability

Every simulation is instrumented with distributed tracing and structured logging. The platform tracks latency distributions, success rates segmented by slippage level and DEX, cache hit ratios, error taxonomy, and per-provider RPC health. Queue depth, rejection rates, and protection block rates are monitored via real-time gauges.

Alerting triggers when key metrics breach operational thresholds, covering simulation latency, error rates, queue saturation, and RPC endpoint health, ensuring the operations team is notified before users experience degradation.

5. The Eleven-Layer Protection Model

GUARD deploys eleven independent protection layers, each targeting a specific loss vector. Layers operate in sequence, with each layer able to independently block a trade or flag it with graduated severity.

Layer 1: Pre-Execution Simulation

The core simulation layer wraps Solana's transaction simulation RPC to test trades before broadcast. Key technical features:

- **Compute Budget Optimization:** Dynamically adjusts compute unit limits per transaction type: distinguishing simple token transfers, standard AMM swaps, and complex multi-hop routes, preventing simulation failure from insufficient budget allocation.



- **Priority Fee Injection:** Network-congestion-aware fee recommendations are injected into each simulation to ensure realistic execution conditions. Without this, simulations at zero fee would pass where paid executions would fail.
- **Slot-Aware Execution:** Always uses the latest confirmed slot for simulation state, ensuring tests run against current blockchain reality, not a stale snapshot.
- **Confidence Scoring:** Each result receives a composite confidence score derived from RPC health, slot lag recency, cache freshness, and historical error patterns. Low-confidence results automatically trigger retries through alternate providers.
- **Predictive Pre-Simulation:** Frequently traded token pairs are pre-simulated during idle cycles, reducing perceived latency for popular pairs.

Layer 2: Token Contract Scanning

Pre-trade contract security analysis integrating three data sources:

1. **RugCheck.xyz API:** Community-vetted risk reports with detailed contract analysis, including token creator history and community safety scores.
2. **Birdeye API:** Token metadata, holder count, creation date, volume history, and price data.
3. **On-Chain Heuristics:** Direct RPC inspection of the token's mint account for mint authority, freeze authority, program upgradeability, and transfer hook analysis.

Risk Flags (9 total):

Flag	Detection Method	Impact
honeypot	RugCheck + simulated sell test	Funds permanently trapped
hiddenTax	Transfer fee extension inspection	Silent value extraction
mintAuthorityActive	On-chain mint account check	Unlimited dilution risk
freezeAuthorityActive	On-chain mint account check	Funds frozen risk
blacklistFunction	Program bytecode analysis	Targeted blocking
proxyContract	Program data inspection	Contract replacement risk
unverifiedSource	Verified build check	No audit possible



GuardApp Corporation

Know Before You Swap

lowLiquidity	Pool account inspection	Extreme price impact
rugPullHistory	Creator address forensics	Previous scam linkage

Risk Response Tiers:

Tier	Criteria	GUARD Action
 Safe	No significant flags	Proceed to simulation
 Suspicious	Minor concerns detected	Warning displayed; proceed with caution
 High Risk	Multiple warning signs	Strong warning; multi-step confirmation required
 Critical	Definitive scam indicators confirmed	Trade blocked; detailed explanation provided

Layer 3: Cross-DEX Route Optimization

Compares execution quality across Jupiter, Raydium, Orca, and other DEXes simultaneously:

1. **Jupiter:** Queries the aggregator's quote API for multiple route options. Each route is simulated independently to verify execution against current pool state.
2. **Raydium:** Direct AMM path simulation against the relevant pool account.
3. **Orca:** CLMM (Concentrated Liquidity Market Maker) path simulation with tick-aware price calculation.

Route Scoring: Routes are scored on a composite of output amount, price impact, fee cost, and route simplicity. The highest-scoring route across all three venues is selected for execution.

Layer 4: MEV & Sandwich Protection

Multi-vector MEV detection:



GuardApp Corporation

Know Before You Swap

- **Known Bot Registry:** A maintained registry of identified sandwich and arbitrage bot addresses, sourced from public MEV research, community reports, and on-chain pattern analysis.
- **Bundle Monitoring:** Real-time mempool data analyzed for sandwich patterns: buy-same-token followed by sell-same-token within tight transaction windows.
- **Pattern Recognition:** Front-run and back-run detection identifies the characteristic two-transaction sandwich structure surrounding the user's intended swap.

MEV Risk Tiers: None, Low, Medium, High, and Critical, escalating from no activity detected to multiple competing bots on the same pool.

Mitigation Strategies: When elevated risk is detected, GUARD can recommend adjusted slippage, route through an alternative venue where the bot is not active, or suggest timing adjustments.

Layer 5: Read-Only Architecture

Not only a detection layer, but a secure read – only architecture. The wallet adapter connection is explicitly read-only. The platform never receives private keys, never requests transaction signing, never holds user funds, and never has custody of tokens. This is architecturally enforced, not a policy promise.

Layer 6: Liquidity Depth Analysis

Pre-trade pool depth verification:

- **Pool State Fetching:** WebSocket subscriptions maintain live account data for tracked pools, ensuring liquidity checks use near-real-time snapshots.
- **Price Impact Calculation:** Computes expected price movement using the appropriate AMM formula for each pool type: constant product for standard pools, tick-aware for concentrated liquidity positions, and per-hop summation for aggregator routes.
- **Threshold Warning:** Trades exceeding safe ratios of trade size to pool depth receive graduated warnings and recommendations to split orders or seek deeper venues.

Layer 7: Slippage Ladder Intelligence

Detailed in Section 3.3. The ladder is enhanced by:

- **Dynamic Level Reordering:** Historical pattern analysis reorders the ladder per token pair to test statistically successful levels first, improving early-stop probability.
- **Smart Cost Estimation:** Gas savings are calculated as the difference between what would have been paid for a broadcast transaction and zero (blocked trades consume no compute budget).
- **Slippage Savings Calculation:** The delta between the user's typical manual slippage setting and the optimal level found by GUARD, multiplied by trade size, is the direct savings per trade.

Layer 8: Whale Watch & Community Alerts

- **Whale Watch:** Tracks wallets holding significant percentages of tracked token supplies, monitoring for accumulation patterns, dumping behavior, and sniper activity. Alerts trigger when relevant whale activity is detected on tokens the user is about to trade.
- **Community Anomaly:** Statistical outlier detection on aggregated trade patterns. Excessive failure rates, unusual volume spikes, and coordinated trading patterns trigger community-wide alerts via Discord and Telegram webhooks.

Layer 9: Encrypted Session Security

Session and application security:

- **JWT tokens:** Short-lived access tokens with longer-lived refresh tokens
- **Device fingerprinting:** Browser/device analysis for session anomaly detection
- **Session revocation:** Per-device logout and full session invalidation
- **MFA/TOTP:** Optional two-factor authentication via authenticator apps
- **CSRF protection:** Token-based CSRF on all mutating endpoints
- **Rate limiting:** On authentication and sensitive endpoints

Layer 10: RPC Redundancy & Failover



GuardApp Corporation

Know Before You Swap

As detailed in Section 4.3, a multi-provider weighted pool with circuit breakers, health scoring, and automatic failover ensures protection remains available even during provider outages or network congestion.

Layer 11: Outcome Feedback Loop

Post-execution verification system:

1. **Prediction Recording:** When a trade is allowed, the simulation's prediction (expected output, slippage, fees) is stored.
2. **Outcome Verification:** Confirmed on-chain outcomes are compared to predictions via WebSocket transaction monitoring.
3. **Accuracy Calculation:** The delta between predicted and actual outcomes feeds the confidence scoring system. Systematic deviations trigger provider re-evaluation and algorithm tuning.
4. **Feedback Integration:** Outcome data refines slippage level ordering, token risk assessments, and MEV detection thresholds. The system improves continuously with every protected trade.

6. Counter-Trade Intelligence (CTI)

6.1 Concept

Counter-Trade Intelligence is a **VIP-exclusive feature** that answers the question: *"Who is on the other side of this trade, and what does their presence mean for my execution?"*

Unlike traditional trading tools that focus only on price and liquidity, CTI profiles the counterparty, the wallet(s) providing liquidity, the arbitrageurs active on the pool, the market makers setting quotes, and any other participants whose behavior could affect trade outcomes.

6.2 Technical Implementation

The CTI system builds counterparty profiles through multi-source data aggregation:



1. **Solscan Transaction History:** Full transaction history for the counterparty address, including all DEX interactions, token transfers, and program invocations.
2. **On-Chain PnL Calculation:** Token balance changes over time mapped to USD value using Jupiter price feeds, producing win/loss ratio and cumulative PnL metrics.
3. **Behavioral Classification:** Wallet type assignment based on transaction patterns, whale (large holdings, infrequent trades), bot (high frequency, pattern-driven), market maker (bid-ask spread capture), retail (small amounts, irregular timing), sniper (immediate post-creation purchases).
4. **Relationship Graph:** Shared pool interactions, token holdings, and transaction timing correlations between wallets expose coordinated activity patterns.

6.3 Risk Pattern Detection (8 Categories)

#	Pattern	Detection Method	Risk Level
1	Known Rugger	Address linked to previous rug pulls through creator/contract forensics	CRITICAL
2	Sandwich Attacker	Front-run + back-run transaction pattern matching	HIGH
3	Deployer Insider	Token creator actively trading their own token	HIGH
4	Flash Loan Exploiter	Address associated with flash loan protocol exploits	HIGH
5	Coordinated Dumper	Multi-wallet synchronized selling pattern	MEDIUM–HIGH
6	Wash Trader	Circular trading pattern for artificial volume	MEDIUM
7	Phishing Victim	Address flagged in known phishing incident databases	LOW
8	Contract Exploiter	Address that previously exploited protocol vulnerabilities	CRITICAL

6.4 CTI Output

For each trade, the CTI system generates:



GuardApp Corporation

Know Before You Swap

- **Counterparty Risk Score:** Aggregate risk rating (0–100) based on detected patterns
- **Counterparty Profile Card:** Wallet classification, age, PnL history, win/loss ratio
- **Relationship Graph:** Visual network map of the counterparty's connections to other known wallets
- **Trade Impact Prediction:** What similar counterparty profiles have meant for trades in the past
- **Safe Trade Size:** Maximum recommended trade amount given the counterparty's historical behavior
- **Alert Feed Integration:** Real-time notifications when a high-risk counterparty is detected

6.5 CTI Capabilities

The Counter-Trade Intelligence system is designed to analyze and classify counterparty wallets in real time. As the platform scales, CTI builds a growing intelligence database that improves with every trade analyzed:

- **Counterparty Risk Scoring:** Each wallet interacting with a user's trade receives a risk score derived from on-chain behavioral patterns, historical associations, and transaction characteristics.
- **Behavioral Classification Engine:** Wallets are classified into categories (whale, bot, market maker, retail, sniper) based on transaction frequency, size distribution, timing patterns, and pool interaction history.
- **Relationship Graph Construction:** Shared pool participation and temporal transaction correlations between wallets are mapped to detect coordinated activity networks.
- **Continuous Learning:** The Outcome Feedback Loop (Layer 11) validates CTI predictions against confirmed on-chain outcomes, progressively refining detection accuracy over time.

7. The GUARD Token: Utility-Driven Economic Design

7.1 Token Overview



GuardApp Corporation

Know Before You Swap

Parameter	Details
Token Name	GUARD
Symbol	GUARD
Blockchain	Solana (SPL Token)
Total Supply	1,000,000,000 (1 Billion): Fixed, no minting
Launch Price	\$0.001 per GUARD
Launch Platform	PinkSale
Launch Date	August 20, 2026

7.2 Token Utility

The GUARD token is a **utility token**: not a governance token, not a revenue-sharing token, not a security. It provides concrete, measurable benefits within the GUARD ecosystem:

1. Subscription Tier Unlock (Primary Utility)

The GUARD token acts as a discount key: holding the required USD equivalent unlocks 50% off the full non-holder price on Pro and VIP tiers. Standard tier requires no token hold.

Tier	Non-Holder Price	With GUARD (50% off)	Token Requirement	Trades/Month	Key Features
Standard	\$8.99/mo	\$8.99/mo	None	30	Basic simulation, slippage ladder, RPC failover
Pro	\$23.98/mo	\$23.98/mo \$11.99/mo	\$50 USD in GUARD	120	+ MEV protection, liquidity analysis, cross-DEX, whale alerts
VIP	\$33.98/mo	\$33.98/mo \$16.99/mo	\$100 USD in GUARD	360	+ CTI, token scanning, honeypot detection, counterparty profiling, priority support



GuardApp Corporation

Know Before You Swap

Non-holders pay the full non-holder price. Token holders unlock the 50% discounted rate. Verification is on-chain: the system checks the connected wallet's GUARD balance at billing time. If the balance drops below the threshold, the subscription reverts to the non-holder price at the next billing cycle.

2. Pay-As-You-Go (PAYG) Overages

When a user exhausts their monthly trade allocation, additional trades are available via PAYG: **\$0.10 USD per trade**, purchased in blocks of 100 (\$10 USD minimum) through the dashboard. Payment is via credit card (USD) through Stripe. Overages are paid in fiat only: GUARD tokens are not consumed for individual trades. Holding GUARD is what unlocks the tier discount, creating sustained holding demand independent of trade volume.

3. Loyalty & Commitment Rewards

Users commit GUARD tokens to the loyalty vault to gain free VIP access periods:

Commitment Duration	\$50 in GUARD	\$100 in GUARD
6+ months	2 weeks free VIP	4 weeks free VIP
1+ year	1 month free VIP	2 months free VIP
2+ years	3 months free VIP	6 months free VIP

- **No lockup:** Tokens can be uncommitted at any time
- **All-or-nothing rewards:** Rewards are earned only when you reach a commitment threshold. If you uncommit before reaching a threshold, no reward is issued. This ensures rewards go exclusively to loyal, long-term holders.
- **No punishment:** Loyalty is rewarded, never penalized

4. Exclusive Access

Token-gated features include custom slippage strategies, advanced analytics dashboards, private community channels (Discord), and early access to new protection modules before public release.

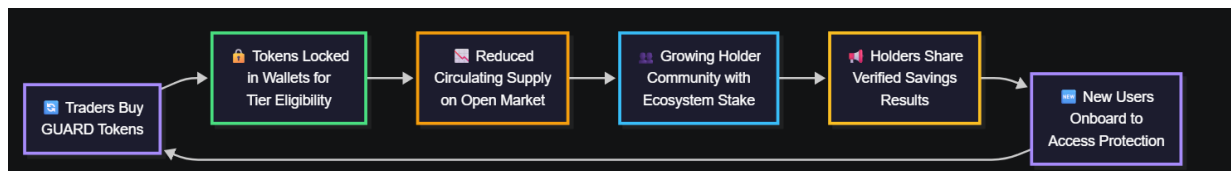


GuardApp Corporation

Know Before You Swap

7.3 The Economic Flywheel

The GUARD token economy operates as a self-reinforcing cycle where each phase naturally drives the next:



How the cycle compounds: Each new user who buys GUARD to unlock a tier removes those tokens from active circulation. As the user base grows, more tokens are held for utility rather than traded. This creates natural scarcity without artificial mechanisms, the token's utility as an access key is what drives holding behavior, and holding behavior is what reduces supply. The platform's subscription revenue ensures the team never needs to sell its allocation, further protecting the cycle from external sell pressure.

7.4 Token Verification

On-chain balance verification is performed through standard Solana RPC calls using the connected wallet's public key. The verification is:

- **Read-only:** The system checks only the GUARD token account balance
- **Non-custodial:** Tokens remain in the user's wallet at all times
- **Privacy-preserving:** No personal data is associated with balance checks

8. Tokenomics: Supply, Distribution & Vesting

8.1 Total Supply Allocation

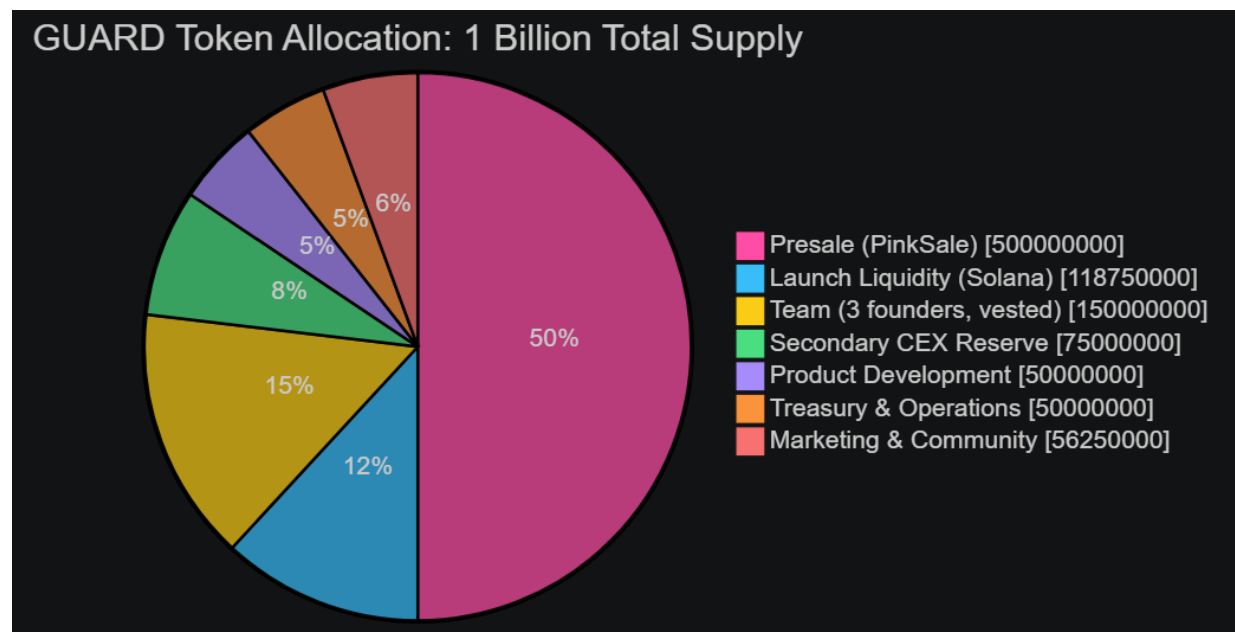
Allocation	Tokens	Percentage	Purpose
PinkSale Presale	500,000,000	50%	Public presale distribution
Launch Liquidity (Solana)	118,750,000	11.875%	Raydium liquidity pool



GuardApp Corporation

Know Before You Swap

Team (3 founders, vested)	150,000,000	15%	Long-term alignment
Secondary CEX Reserve	75,000,000	7.5%	Future centralized exchange listings
Product Development	50,000,000	5%	Engineering and R&D
Treasury & Operations	50,000,000	5%	Operating expenses, legal, compliance
Marketing & Community	56,250,000	5.625%	Growth, KOL outreach, community building
Total	1,000,000,000	100%	



8.2 PinkSale Presale Structure

Metric	Soft Cap	Hard Cap
Total Raise	250,000 USDC	500,000 USDC
PinkSale Fee (5%)	12,500 USDC	25,000 USDC
Net Proceeds	237,500 USDC	475,000 USDC



GuardApp Corporation

Know Before You Swap

Metric	Soft Cap	Hard Cap
Liquidity (25% of net)	59,375 USDC	118,750 USDC
GUARD for Liquidity	59,375,000 (5.9375%)	118,750,000 (11.875%)

Launch Price: \$0.001 per GUARD (same for both scenarios)

Platform: PinkSale (leading Solana launchpad)

Soft Cap Protection: The soft cap of **250,000 USDC** is the minimum viable raise. If the presale does not reach this threshold, **all funds are automatically returned** to participants via PinkSale's refund mechanism. There is no scenario where the project receives partial funding without the means to deliver: either the soft cap is met, and the platform is fully funded, or every participant gets their USDC back.

8.3 Vesting & Lock Schedule

Presale Buyers:

- 20% unlocked at Token Generation Event (TGE)
- 6-month cliff (no tokens released)
- Months 7–10: 20% released each month (linear)
- Full unlock: Month 10
- Buyers must manually claim each unlock on PinkSale

Team Allocation:

- 12-month lock from TGE
- Linear vesting over 24 months following the lock
- Total vesting period: 36 months

Liquidity Pool:

- Locked for 12 months from launch
- Verifiable on-chain through the DEX liquidity lock contract



GuardApp Corporation

Know Before You Swap

8.4 Key Protection Mechanisms

1. **No Inflation:** Fixed 1 billion supply. No mint function exists. No additional tokens can ever be created.
2. **Team Vesting:** Three-year alignment ensures founders are incentivized for long-term platform success, not short-term token price.
3. **Liquidity Lock:** 12-month lock prevents any possibility of a liquidity rug pull during the critical first year.
4. **Self-Sustaining Revenue:** Operating costs are funded by subscription revenue, not token sales. The team never needs to sell its allocation to fund development (see Section 9).

9. Revenue Model & Economic Sustainability

9.1 Revenue Streams

GUARD generates revenue through two channels:

1. **Monthly Subscriptions:** Recurring revenue from Pro (\$11.99/mo) and VIP (\$16.99/mo) tiers
2. **Pay-Per-Trade Overage:** \$0.10 per trade beyond monthly allocation, sold in blocks of 100

GUARD does not take a percentage of trades, charge per-transaction fees on protected trades, or monetize user data.

9.2 Unit Economics

The core cost driver is RPC calls to Solana nodes. Each simulation (5 parallel levels + pre-checks) consumes approximately 8–12 RPC calls. With caching (40–60% hit rate), effective calls per trade are reduced to 4–7.

Per-Trade Cost:

- RPC calls (worst case, no cache): \$0.0008–\$0.0012 per trade



GuardApp Corporation

Know Before You Swap

- RPC calls (typical, 50% cache): \$0.0004–\$0.0006 per trade
- Infrastructure (amortized): \$0.0002 per trade

Per-User Revenue vs. Cost (VIP tier, 360 trades/month):

- Revenue: \$16.99/month
- RPC cost (typical): ~\$0.18/month
- Infrastructure cost (amortized): ~\$0.07/month
- Margin: >98%

9.3 Scaling Trajectory

Stage	VIP Subscribers	Monthly Revenue	Monthly RPC Cost	Monthly Margin
Early Traction	500	~\$8,500	~\$150	>98%
Growth	5,000	~\$85,000	~\$1,500	>98%
Scale	10,000	~\$170,000	~\$3,000	>98%
Mature	50,000	~\$850,000	~\$15,000	>98%

The margin remains near-100% at every scale because the marginal cost of an additional simulation is effectively zero, the RPC infrastructure is shared and the primary cost is fixed infrastructure, not per-transaction fees.

9.4 Self-Sustaining Operations

A critical architectural property: **the team never needs to sell tokens to fund operations.**

The PinkSale presale is a one-time capital event that funds the initial build, launch, and marketing push. After launch, the platform runs entirely on recurring subscription revenue, which is cash-flow positive from the first paying user. This has three profound implications:

1. **No sell pressure from the team.** The founding team's 15% allocation is held for long-term alignment, not liquidated to pay salaries.



2. **Subscription revenue scales with users, not token price.** Even if the token trades at launch price indefinitely, the platform remains profitable and growing.
3. **Runway independence.** Monthly operating costs are a fraction of monthly subscription revenue at any user count above approximately 50 paying subscribers.

10. Competitive Landscape & Market Opportunity

10.1 The Solana DEX Market

Solana consistently ranks among the top three blockchains by DEX volume, processing billions in daily swaps. The ecosystem includes:

- **Retail traders:** 10–1,000+ trades per month, the primary GUARD user base
- **Memecoin traders:** High-risk, low-liquidity pairs where protection is most valuable
- **Airdrop farmers:** High-volume strategies where per-transaction costs compound
- **On-chain analysts:** Need execution quality transparency

10.2 Competitive Gap Analysis

Capability	GUARD	Jupiter	Birdeye	RugCheck	Phantom
Pre-Execution Simulation	☑	✗	✗	✗	✗
5-Level Slippage Ladder	☑	✗	✗	✗	✗
Token Contract Scanning	☑	✗	✗	☑	✗
Honeypot Detection (Buy+Sell Sim)	☑	✗	✗	Partial	✗
MEV & Sandwich Detection	☑	✗	✗	✗	✗
Multi-DEX Route Comparison	☑	☑	✗	✗	✗
Counter-Trade Intelligence (CTI)	☑	✗	✗	✗	✗
Whale Watch & Sniper Detection	☑	✗	☑	✗	✗

**GuardApp Corporation**

Know Before You Swap

Capability	GUARD	Jupiter	Birdeye	RugCheck	Phantom
Gas Fee Savings (Blocks Failed TxS)	☑	✗	✗	✗	✗
Liquidity Depth Analysis	☑	✗	✗	✗	✗
RPC Redundancy (7 endpoints)	☑	N/A	N/A	N/A	✗
Community Anomaly Alerts	☑	✗	✗	✗	✗
Multichain Roadmap	☑	✗	✗	✗	✗

GUARD is the only platform that combines all of these protections in a single unified tool. It is not an incremental improvement over existing options, it defines a new category: **pre-execution transaction protection**.

10.3 Market Timing

Three converging trends create the moment for GUARD:

1. **Retail adoption acceleration.** Lower barriers to entry, improved mobile wallets, fiat on-ramps, simplified interfaces, are bringing traders who expect consumer-grade protection.
2. **MEV industrialization.** As Solana DeFi grows, MEV extraction becomes more sophisticated, automated, and profitable. The window for building protective infrastructure is now.
3. **Scam token proliferation.** Thousands of new tokens launch daily via platforms like Pump.fun. Many are scams. Manual research is impossible at this scale. Automated screening is necessary.

10.4 Multichain Expansion

GUARD's simulation engine is chain-agnostic. The same simulateTransaction pattern, the same 11-layer protection model, the same token scanning and MEV detection logic, all of it generalizes to any blockchain that supports pre-execution transaction simulation through standard RPC interfaces. Solana is the launch chain. Ethereum and Base integration are on the roadmap, multiplying the addressable market while reusing the same core technology.



11. Roadmap

Phase 1: Foundation (Complete ☒)

- Core simulation engine: 5-level slippage ladder with parallel execution
- Multi-provider RPC pool (7 endpoints) with health scoring and circuit breakers
- User dashboard with real-time trade protection and savings tracking
- Wallet connection (read-only) with Phantom, Solflare, Backpack support
- Token Contract Scanner: RugCheck + Birdeye + on-chain heuristics
- MEV Detector with 20+ known bot address registry
- Cross-DEX Route Optimizer (Jupiter, Raydium, Orca)
- Stripe subscription integration with tier management

Phase 2: Token Launch (Current)

- GUARD SPL token creation and PinkSale presale configuration
- Token-gated subscription tier system
- On-chain GUARD balance verification
- Jupiter price oracle for token valuation
- Pay-per-trade overage system
- Raydium liquidity pool creation
- Presale buyer vesting contract

Phase 3: Full Protection Rollout

- Complete all 11 protection layers to production readiness
- Counter-Trade Intelligence (CTI) with full 8-pattern detection
- Whale Watch with real-time alerting
- Honeypot Detector: simulated buy + sell transaction pipeline
- Community Anomaly Detection with Discord/Telegram webhooks
- Outcome Feedback Loop: prediction vs. actual verification
- Historical Pattern Learner: ML-driven ladder reordering
- Institutional API access via API key management



- Advanced analytics dashboard with export capabilities

Phase 4: Security & Scale

- Third-party smart contract audit (SolidProof or equivalent)
- Penetration testing: injection, auth bypass, rate-limit bypass, webhook replay
- Dependency vulnerability remediation: target 0 critical, 0 high
- Performance optimization: sub-100ms average simulation latency
- Global RPC endpoint distribution for geographic latency reduction
- Redis distributed caching (beyond current in-memory LRU)
- Horizontal scaling architecture: simulation workers as independent serverless functions

Phase 5: Multichain Expansion

- Ethereum simulation engine: EVM-compatible pre-execution validation
- Base L2 integration
- Cross-chain protection: unified dashboard across all supported chains
- Chain-specific MEV detection (Ethereum PBS/MEV-Boost, Base sequencer analysis)
- Multichain token utility: GUARD token bridges to new chains
- The same simulation engine, now protecting trades across every major ecosystem

Gantt Timeline View — Each = 1 Quarter								
	Q1 2026	Q2 2026	Q3 2026	Q4 2026	Q1 2027	Q2 2027	Q3 2027	Q4 2027
Phase 1 — Foundation								
Phase 2 — Token Launch								
Phase 3 — Full Protection								
Phase 4 — Security & Scale								
Phase 5 — Multichain								

12. Security Architecture & User Protection

12.1 Architectural Security Guarantees

GUARD's security model is based on **architectural constraints**, not policy promises:



- **Read-Only Wallet Connection:** The Solana wallet adapter is initialized with `signTransaction: false`. This is enforced at the protocol level, GUARD literally cannot construct a signed transaction, even if its code were compromised.
- **No Private Key Surface:** Private keys, seed phrases, and derivation paths never enter GUARD's domain. They exist only in the user's wallet software.
- **No Custody:** At no point does GUARD hold, escrow, or intermediate user funds or tokens. All token holding verification is on-chain; all tokens remain in user wallets.

12.2 Data Protection

- **AES-256-GCM Encryption:** Session data, MFA secrets, and sensitive fields are encrypted at rest
- **HMAC-SHA256 Request Signing:** API calls include cryptographic signatures with nonce-based replay protection
- **Immutable Audit Logs:** SHA-256 hash-chained audit trail, tampering with any entry invalidates the entire chain
- **Data Minimization:** Only data essential to the service is collected. No PII is required beyond an email address for subscription management
- **PostgreSQL Encryption:** PII fields encrypted at the database level using pgcrypto
- **PIPEDA Compliance:** As a Canada-based project, GUARD adheres to Canadian federal privacy law
- **GDPR-Ready:** Data export and erasure available from user Profile settings

12.3 Infrastructure Security

- **HTTPS Enforcement** with HSTS headers (`max-age=31536000`, `includeSubDomains`, `preload`)
- **Content Security Policy 2.0:** Nonce-based CSP with Trusted Types enforcement prevents DOM XSS
- **30+ Permission Policy Directives:** Explicitly deny sensitive browser features (camera, microphone, geolocation, etc.)
- **CORS Locked:** Restricted to production domains only



- **Stripe Webhook Signature Verification:** Mandatory in production, prevents webhook forgery
- **Rate Limiting:** Per-IP and per-endpoint on all API routes
- **CSRF Protection:** Token-based on all mutating endpoints
- **Dependency Scanning:** Automated vulnerability scanning in CI/CD pipeline
- **Secrets Audit:** No secrets in repositories, logs, or client bundles

12.4 KYC & Audit

- **Team KYC:** All three founders are KYC-verified through PinkSale
- **Smart Contract Audit:** Third-party audit (SolidProof or equivalent) before public launch
- **Automated Testing:** 270+ tests covering simulation engine, protection layers, and API endpoints

13. Team

GUARD is built by a three-founder team based in Canada, combining deep technical expertise with go-to-market execution capability.

Role	Focus Areas
Chief Executive Officer	Vision, strategic direction, go-to-market execution, investor relations. A seasoned leader with experience building companies from the ground up.
Chief Technology Officer	Simulation engine architecture, Solana development, infrastructure, security, token program. Architected the entire GUARD platform including all 31-engine subsystems, 11 protection layers, and production infrastructure.
Chief Operating Officer	Operations, compliance, legal, partnerships, community management. Has run operations before and knows how a company at this stage should function.



The founding team collectively holds 15% of the total token supply (150,000,000 GUARD), vested over 36 months (12-month lock + 24-month linear vesting). This aligns long-term incentives: the team benefits only if the ecosystem grows and the token has sustained utility.

14. Risk Factors & Disclaimer

14.1 Market Risks

- **Cryptocurrency markets are volatile.** The value of GUARD tokens may fluctuate significantly based on market conditions, adoption rates, and broader crypto market trends.
- **Subscription demand is unproven at scale.** While unit economics are compelling for individual traders, aggregate demand across thousands of users has not been market-tested.
- **Competition may emerge.** First-mover advantage provides a window, but competitors with greater resources could enter the market.

14.2 Technical Risks

- **Simulation accuracy depends on RPC quality.** If RPC providers return stale or incomplete state, simulation results may not match on-chain outcomes. The multi-provider pool and caching layers mitigate but do not eliminate this risk.
- **The Token Contract Risk Scanner has inherent limitations.** Static bytecode analysis and heuristic checks cannot detect all scam patterns. Novel attacks, social engineering, and non-code-based exploits fall outside its detection scope.
- **Solana network upgrades may require protocol adaptation.** Changes to the Solana runtime, transaction format, or RPC API could necessitate engineering work.
- **MEV detection is pattern-based, not exhaustive.** New MEV strategies and previously unidentified bot addresses may evade current detection methods.



GuardApp Corporation

Know Before You Swap

14.3 Regulatory Risks

- **The regulatory landscape for blockchain tokens is evolving.** Classification of utility tokens varies by jurisdiction. Changes in regulation could affect GUARD's operation or the token's tradability.
- **PinkSale presale participants should understand the risks** of early-stage token purchases, including potential illiquidity and price volatility.

14.4 Disclaimer

This white paper is an informational document describing the GUARD platform, its architecture, its tokenomics, and its roadmap. It is not:

- An offer or solicitation to purchase securities
- A promise of future value, returns, or performance
- A guarantee that the platform will achieve specific protection rates, user numbers, or revenue figures
- Investment advice of any kind

The GUARD token is a utility token designed to unlock subscription tiers and access features within the GUARD ecosystem. Its value is derived from the utility it provides. Prospective purchasers should evaluate the platform's merits independently and consult qualified professionals regarding legal, tax, and financial implications.

15. Conclusion

The Solana ecosystem has achieved remarkable technical scale. Four hundred millisecond blocks. Sub-cent fees. Billions in daily DEX volume. But the infrastructure that protects individual traders has not kept pace with the infrastructure that moves their money.

Every day, value drains from the ecosystem through vectors that are well-understood, measurable, and preventable:

- Failed transactions that charge gas without delivering execution



GuardApp Corporation

Know Before You Swap

- Excessive slippage that silently bleeds 1–5% from every trade
- MEV sandwich attacks that extract hidden value at the trader's expense
- Scam tokens, honeypots, hidden taxes, mint authorities, rug pulls, that trap and destroy capital
- Suboptimal DEX routing that leaves better prices on the table
- Low-liquidity pools that create extreme price impact
- Whale manipulation that crashes positions mid-execution
- Unknown counterparties whose track records would warn any informed trader away

These are not mysteries. These are not unsolvable problems. They are engineering failures, failures that GUARD was built to fix.

GUARD is not a trading strategy. It is not a signal service. It is not a get-rich-quick promise. It is **infrastructure for protection**: a simulation-first execution layer that sits between the trader and the blockchain and answers, for every trade, the eight questions that determine whether value is created or destroyed.

The numbers are verifiable. A trader saving \$15 per trade on 100 trades monthly saves \$1,500, recorded, displayed, and proven against their own wallet history. Against a subscription that costs less than a single saved trade, the value proposition is self-proving.

The GUARD token is the key that unlocks this protection at its best possible price. It is a utility, not a speculation, and it pays for itself on the very first trade.



GuardApp Corporation

Know Before You Swap



GUARD: Know Before You Swap

guardapp.ca · [X / Twitter](#) · [Discord](#) · [Telegram](#)

[YouTube](#) · [TikTok](#) · [Instagram](#) · [Facebook](#)

© 2026 GUARD. All rights reserved. Built on Solana.