



OpenSentry

Audit-grade smart contract
protection for individuals.

The Invisible Risk

Every blockchain interaction requires trusting code.

But most users only see a "**Confirm Transaction**" button.

Behind that button may be exploit paths that they don't understand.

Today only well-funded protocols and enterprises receive professional security audits.

Individual users interact with all kinds of contracts **without protection.**

Why Current Solutions Fail

Existing wallet protections rely on blacklists and reputation scores.

They detect **known scams**, but not **structural risk**.

Users still cannot answer:

"What could happen to my assets in the future if I sign this?"

The Insight

Professional auditors detect risk by:

Exploring
execution paths

Modeling exploit
scenarios

Analyzing
privilege surfaces

This methodology has **never been applied directly to end users.**

OpenSentry brings **audit logic to the wallet layer**, shifting security from protocol teams to individual users.

Users can feel safe interacting with **any protocol** since they are keeping security in their own hands.

The Technology

OpenSentry analyzes a contract like an auditor would.

It combines:

- smart contract line-by-line code analysis
- static analysis
- symbolic execution
- exploit pattern detection
- business logic and financial logic verification
- access control verification
- execution path simulation

It then generates **plain language risk explanations.**

Example User Warning

Before
OpenSentry

"Request may
not be safe."

With OpenSentry

- "Depositing funds could result in losing your accumulated interest in the future if the contract is compromised."
- "All your deposited funds could be withdrawn at any time by the contract's admin, make sure you trust this protocol."
- "Withdrawing from this contract would result in receiving 0.00048 ETH (\approx \$7) less than is owed, due to a rounding error."

Users see **clear consequences**, in language they can understand.

Impact

OpenSentry **democratizes audit-level protection.**

-  Prevents avoidable losses
-  Increases trust in decentralized systems
-  Expands safe participation in Web3

In blockchain, where individuals hold custody of their own funds, they should also be in charge of their own security.

OpenSentry allows users to bring their own protection when interacting with web3 protocols.

Roadmap

Now-Q2 2026: Core Engine
(In Progress)

Building the foundational analysis and exploit detection capabilities

Q4 2026: wallet extension

building the Metamask wallet extension

1

2

3

4

Q3 2026: Early User Testing

Launching a public Beta standalone tool for testing and gathering feedback by early users

Q1 2027: API & Developer Access

Empower devs with an open-source API

Thank you!

Liron Achdut

Founder

Smart contract auditor and activist

Feel free to contact me :)

Telegram: **@lirona1**