What is the Webacy Risk Data Network?

Webacy is a risk data network that helps wallets & applications protect their users against scams, hacks, and mistakes across the blockchain.

Wallets, protocols, & applications use Webacy throughout their user experience:

Address trust and safety

- Assess the safety of interacting with a given address (any address: EOA, smart contract, token, etc.). Screen for blocklists, sanctioned addresses, malicious behavior, and other potential flags
- Analyze smart contract code in real-time
- Filter spam and sybil addresses

Connected wallets

- Block sanctioned addresses and wallets involved in malicious behavior
- Educate users with a Wallet Safety Score
- Delight users by enabling additional features or providing additional value
- Display open approvals and the risks associated

Before a transaction

- Block harmful dApps and links
- Review address trust and safety prior to signature
- Protect users from interacting with malicious smart contracts

Monitoring and Notifications

- Monitor all on-chain activity associated with your protocol or smart contracts
- Enable wallet monitoring and flag for risky transactions
- Proactively notify users (or be notified) of any potentially risk activity involved with a given address

Get started with Webacy

Start building in minutes:

- Reach out toinfo@webacy.com
- for an API key
- Check out theQuick Start Integration Guide

APIs

Webacy's APIs are REST-based APIs that expose your platform to Webacy's Risk Engine and Wallet Watch Notifications Platform.

With over 15+ data providers, along with their data analytics and algorithms, Webacy has the broadest risk coverage across the blockchain ecosystem. From compliance and regulatory data to social engineering scams and crowdsourced reports, they process millions of monthly signals, updating their models with the latest and most up-to-date information.

For detailed technical documentation and to begin testing the APIs directly, visit theitechnical documentation . Available APIs and corresponding use cases include:

Threat risks API

This API indicates if a given address is a risk or a threat to others. It returns risk data associated with the supplied address. It flags if the address appears in any sanctioned databases, has been historically flagged as malicious, is associated with a scam smart contract, and so on. It also includes filtering for spam/sybil signals.

Some common use cases for this endpoint include:

- Filtering addresses for spam
- Blocking high-risk addresses from utilizing your service
- Presenting high-risk addresses to others as potentially risky to interact with
- Protecting your platform by restricting high-risk addresses

Approval risks API

This API returns a list of approvals for a given address and the associated risk of the spender for that approval. Approvals are commonplace in crypto - now you know which ones put you at risk. Check out your open approvalshere .

If you're a wallet interested in native revoke and approval risk scoringreach out to Webacy .

Transaction risks API

This API returns risk data for a given transaction. Pass in any transaction hash, and the API will return a risk score result that incorporates counterparty EOA risk profiles, address risk, involved asset smart contract risk, and more.

Some common use cases for this endpoint include:

- Understanding the historical behavior of an address
- Providing data to give recommendations about on-chain activity
- Gaining insight into a particular transaction or action
- Flagging previously unknown activity that was potentially at risk

Exposure risk API

The original Webacy Safety Score, this API returns a 'risk profile' or 'exposure risk' of a given address.

This indicates the exposure the address has to risky activity through historical transactions, behavior, and owned assets. This endpointdoes not assess whether the supplied address is a risk to others (Threat Risk). Instead, it assesses whether the supplied address isat risk from others.

Some common use cases for this endpoint include:

- Gaining a holistic understanding of a client or personal wallet
- Enabling recommendations and analysis on past behavior
- Assessing common traits of a user base
- Determining types of users to better serve them
- Triggering warnings to internal teams or external users based on changes in risk profile based on ongoing activity
- Understanding the behavioral activity of a user base

Check out your risk exposurehere .

Contract risk API

This API returns a contract risk analysis for a given contract address.

The on-demand analysis leverages multiple techniques, such as fuzzing, static analysis, and dynamic analysis, for real-time smart contract scanning.

Some common use cases for this endpoint include:

- Scanning contracts before listing them on your site
- Verifying that you are not promoting malicious contracts
- Checking a contract before interacting with it
- Reviewing code as you build
- Assessing your contracts before submitting them for a formal audit process

URL risk

Given a URL, this endpoint analyzes its safety. It helps you determine if a given link is a phishing scam, sending you to a dangerous place, or is otherwise malicious.

Some common use cases for this endpoint include:

- Assessing the safety of a dapp/website
- Warning your end-users from interacting with a potentially malicious website
- Blocking websites

Wallet watch API

These APIs enable you to register users to Webacy's real-time notification infrastructure.

If you're interested in setting up your own private instance with custom messaging and triggerscontact us . Edit this page
Last updatedonJan 27, 2025 Previous Venly Next Contribute docs