

ORWOX WHITEPAPER

Official Technical Documentation
Version 1.0 — Updated 2026

Introduction

Orwox is a privacy-focused digital infrastructure project designed to protect internet users from surveillance-based platforms, intrusive advertising networks, malicious software ecosystems, and centralized control over online services. Modern internet platforms rely heavily on collecting user data, tracking browsing activity, and building behavioral profiles for targeted advertising. Orwox was created as an alternative vision for the internet where user privacy and autonomy are prioritized. Full details are available at <https://whitepaper.orwox.com>

Project History

Orwox officially began development on November 11, 2024. The project emerged during a period when internet freedom discussions intensified in Türkiye, particularly following restrictions placed on major communication platforms such as Discord. These events highlighted how vulnerable centralized digital platforms are to regulatory control and infrastructure dependency. Orwox was created as an experimental privacy-focused technology project aimed at developing tools that help users regain control over their digital environment.

Mission

- Protection from intrusive advertising networks
- Protection from malicious software ecosystems
- Reduction of tracking systems
- Improved user anonymity

Technology Overview

The Orwox ecosystem includes several privacy-focused technologies designed to improve internet security, device protection, and network performance. These technologies are integrated into different Orwox products including browser extensions, network utilities, and privacy-focused desktop tools.

- Network optimization tools
- Privacy protection technologies
- Device security utilities
- Ad blocking systems
- DNS protection

DPI Bypass Technology

Deep Packet Inspection (DPI) is a network analysis technology used by internet providers and network operators to inspect and classify internet traffic. Orwox technologies include mechanisms designed to reduce the effectiveness of DPI analysis through packet fragmentation, protocol obfuscation, and DNS routing strategies.

COV: Advanced Privacy Engine

COV fixes the fundamental lack of privacy in the modern internet by rewriting how traffic moves through the network. AI-optimized DNS routing, adaptive MTU tuning, and military-grade DPI bypass work together to make connections faster, safer, and invisible to surveillance systems.

- AI-driven DNS & MTU optimization for peak speed
- Military-grade DPI bypass & packet encryption
- Real-time dark web monitoring & breach detection
- True zero-knowledge — no user data is ever seen

Data Philosophy

Orwox follows a strict minimal-data philosophy. Required system identifiers are stored using cryptographic hashing, ensuring that no meaningful user data exists even if infrastructure is compromised.

Funding Model

Orwox currently operates as an independent project, does not charge users, and accepts voluntary cryptocurrency donations. Total revenue since inception is approximately 43 USD, fully reinvested into development and infrastructure.

Founder

Orwox was founded by Powni, an independent developer focused on privacy and security. The project was started to address the internet's lack of privacy. All development and revenue are reinvested into infrastructure, product improvements, and user empowerment.