


NØNOS



Zero-Trust OS

 nonos.systems

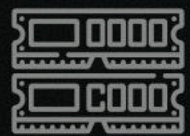
Secure by design. Private by default.

Index

Executive Summary	03	Vision	11
Market Size	04	Economy and Platforms	12-13
The Problem	05-07	Commercialization	14-17
The Solution	08-09	Revenue Trajectory	18
Core Features	10	Team/Advisors & Partners	19-20

Executive Summary

World's First Zero-Trust, Rust-Built OS



Runs entirely in memory
(no trace, no leaks)



Built-in anonymous
networking & Ethereum wallet

Operating Systems

**Our Greatest
Security Risk**

Operating System Industry

Market Size

\$1.93B
Crypto Stolen
In the last 6 months

2 Billion
Computers Worldwide

6,700+
OS Vulnerabilities 2024
(+61% YoY)

\$334B
Hardware
Market 2030

334k
Monthly Tails Users

\$87B (2024)
↓
\$135B (2032)
Global OS Market

71%
Windows Users

72%
Android Users

The Problem

Operating Systems

Operating Systems - The Weak Link

In 2024, Windows logged 1,360 vulnerabilities and macOS 527, with exploited flaws up 30%. Both ship with tracking and bloatware pre-installed, creating attack surfaces.

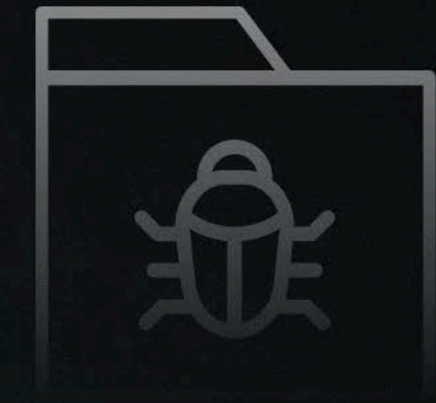
Android adds another layer of risk, with malicious apps scraping memory for banking logins, customer numbers, and 2FA codes. Clipboard malware like MassJacker has already hijacked 778k+ crypto wallets, stealing millions.



Windows & macOS is bloated, insecure, tracking-heavy



Memory exploits
70%+ OS vulnerabilities



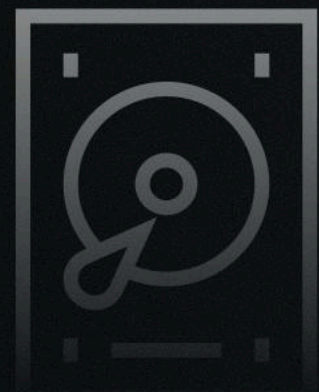
Clipboard and screenshot
malware steal crypto



AI integrations create
new attack vectors

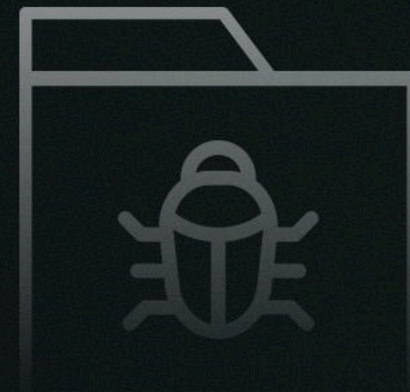
The Problem

Memory & Disk



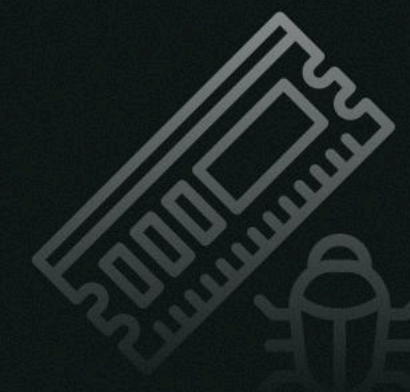
Constant Disk Writes

- Windows & macOS store logs, caches, telemetry, swap files
- Data is never truly deleted → forensic recovery possible



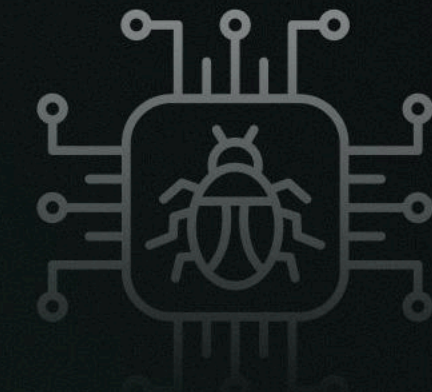
Persistent Attack Surface

- Malware survives reboots by hiding in disk storage
- Sensitive information remains long after sessions end



Unprotected Memory

- Apps read clipboard, keystrokes, and screenshots freely
- Crypto wallets & banking data stolen directly from RAM



AI-Driven Exploits

- Modern attacks target memory & disk simultaneously
- OS designs from decades ago can't defend against this.

The Problem

Network & Wireless

Network & Wireless – The Privacy Breach

Public and untrusted networks expose users to stealthy network attacks such as rogue Wi-Fi hotspots, captive-portal hijacks, and DNS manipulation let attackers intercept traffic and harvest login credentials.

Mobile and desktop devices auto-connect to seemingly legitimate networks, giving adversaries a direct path to steal banking and exchange logins, session tokens, and 2-factor codes.



DDoS and
downtime risks



Centralized networks =
censorship & surveillance



No built-in anonymity in
current operating systems



DNS leaks expose every
site you visit

The Solution

NØNOS Operating System

	Rust Microkernel Memory-safe		RAM-only Zero trace
	Encrypted Mesh Decentralized		Web3-ready ETH wallet + zkAuth

NØNOS Terminal

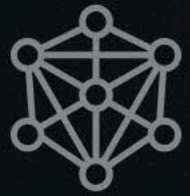
```
NØNOS ZeroState Boot v1.0.0
Loading capability-authenticated syscalls...
Starting Anyone SDK integration...
RAM-resident execution: ACTIVE
Zero-trust verification: PASSED
```

```
System Architecture:
├─ UEFI Bootloader
├─ Rust Microkernel
├─ Syscall Router
├─ vault.rs (crypto)
├─ net.rs (Anyone SDK)
└─ modules/ (sandboxed)
```

```
Anonymous networking ready.
nonos@zerostate:~$
undefined
█
```

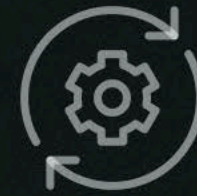
United in Privacy. Built for Security.

NØNOS + Anyone SDK



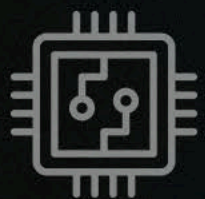
Decentralized Privacy Layer

Routes traffic through multiple encrypted relays, making tracking and surveillance nearly impossible.



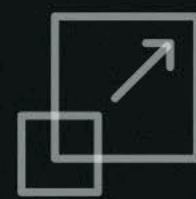
Easy Integration

Drop-in SDK developers can embed into apps, browsers, or operating systems.



Resilient Performance

Balances privacy and speed, ensuring secure connections without degrading user experience.



Scalable & Flexible

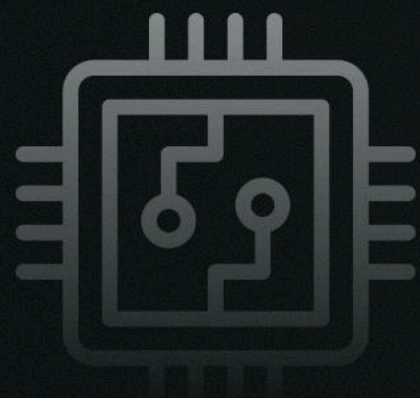
Supports consumer apps, enterprise tools, and blockchain/Web3 ecosystems without central points of failure.



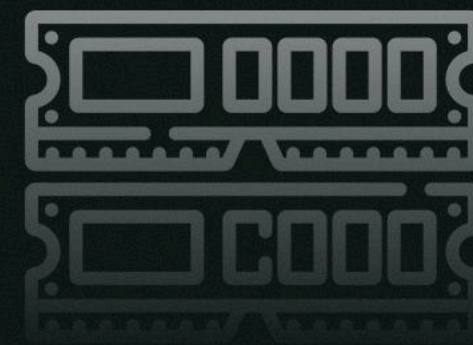
NØNOS and the Anyone SDK deliver A defense-in-depth solution, fusing physical security at the device level with unmatched network security for end-to-end protection.

End-to-End Security. No Gaps.

Core Features



Pure Rust
no unsafe code



RAM-Resident OS
stateless & ephemeral



Ethereum Wallet
built-in, cold-wallet secure



Host Sites/Apps
via Anyone SDK



Encrypted USB persistence
(optional)

Future-Proofing Tomorrow

Vision for the Future

Universal Access to
Secure Private Computing

Crypto and Banking Safely
Anywhere

Trusted Endpoints
Through Secure Devices

“Sovereign computing
is the new standard

\$NOX token fuels
microtransactions (on L2).

Users earn \$NOX by
contributing resources

Scaling Securely

Built-In Economy

Pay relays for bandwidth,
hosting, storage

Powered by
Ethereum / L2 chain

Any Device. Anywhere.

Boot Platforms

ARM

Powering everything from Raspberry Pi to PinePhone, Librem 5, and modern servers. NONOS can extend into this ecosystem to capture developers, privacy enthusiasts, and lightweight edge devices.

Mobile

Android-based and privacy-first phones offer the next frontier. With unlocked devices, NONOS can deliver diskless, RAM-only security to the world's largest computing platform.

Intel / x86_64

The global standard for desktops, laptops, and servers. NONOS boots directly from USB on these systems, providing immediate reach into enterprise and consumer markets.


Apple


Intel Macs: Fully supported with USB boot.



Apple Silicon (M-series): Strategic ARM target, opening the door to high-end users and professional markets.

Personal & Retail

Linux Commercialization

Free OS  Drive Adoption

 Encrypted USB **\$50** Retail



 At 1% of Linux Users  \$0 direct revenue

Offering:
Free version to seed the market and build a global user base.

Target:	Revenue:
Millions of personal users seeking security and privacy.	Growth funnel for Pro, Encrypted USB, and Enterprise upgrades.

Est Revenue:

At a conservative 1% of Linux-scale adoption, NØNOS would onboard 600k–800k active users worldwide (from the 60–80M Linux desktop base). This tier delivers \$0 direct revenue, but builds the funnel for monetisation in paid tiers.

 1% of Linux Users  \$10–20 million/year

Offering:
Plug-and-play personal privacy device with optional persistent storage. Cloud integration. Erased on reboot for malware and virus protection.

Target:	Revenue:
Home users, privacy enthusiasts, crypto users.	Direct retail sales, consumer channel distribution.

Est Revenue:


If each of those users purchased a device, retail demand would equal \$30–40 million per cycle (~ every 2–3 years), averaging \$10–20 million per year. Demand would be driven by privacy-conscious individuals in Linux-strong markets such as the EU, Asia, and North America.


Pro & Enterprise

Linux Commercialization

\$10 / Month / Device  Pro Version

 Enterprise **Bulk Licensing**

 At 1% of Linux Users

 \$72–96 million/year

Offering:
Advanced edition for regulated industries with custom device builds. Diskless design, erased on reboot, live cloud apps.

Target:
Finance, defence, healthcare, and military businesses.

Revenue:
Recurring SaaS revenue per device at scale.

Est Revenue:
At 1% of Linux-scale adoption, the Pro subscription could generate \$72–96 million in recurring annual revenue, with diskless, reboot-erased security as its key differentiator.

 At 1% of Linux Users

 \$144–192 million/year

Offering:
Corporate and government deployments with secure network integration. Includes optional 2FA wizard on boot to prevent misuse of lost devices.



Target:
Governments, enterprises, NGOs.

Revenue:
Large volume licensing + long-term support contracts.

Est Revenue:
With 1% adoption from the same Linux-scale base, enterprise licensing could produce \$144–192 million per year, underpinned by long-term contracts that emphasise compliance, security, and operational resilience.


Personal & Retail

Global Potential

		 Drive Adoption (Free OS)	 Encrypted USB (Consumer Hardware)
Market	Target: Stats:	~2B Devices: Desktops, Laptops, Mobiles Windows ~1.6B devices 2024	~50M+ TAM: Security/crypto devices Yubico ~1M keys/month
Year 1	Target: Revenue: Stats:	~1M Users \$0 (free OS for publicity) Ubuntu Kylin 1.3M installs/6mo	200–400k ~\$5M Trezor 2.4M units 2024
Year 3	Target: Revenue: Stats:	~5M Users \$0 (free OS for publicity) Ubuntu ~13M users in 5y	500K Units ~\$25M Ledger 1M sold in 8mo
Year 5	Target: Revenue: Stats:	~15M Users \$0 (free OS for publicity) Long-term funnel → Paid OS	1.5M Units ~\$75M Ledger 6M lifetime sales

Pro & Enterprise

Global Potential

		 Pro Version (Paid OS)	 Enterprise (B2B/B2G)
Market	Size	100M+ Users	30K+ Orgs
	Evidence	ProtonMail 100M accounts 2023	Red Hat 33K clients
	Stats:	Privacy-focused market	Fortune 500 companies
Year 1	Target:	50K Paid	10 Clients
	Revenue:	~\$6M	\$3–4M
	Stats:	Early free-to-paid converts	Pilot government/enterprise trials
Year 3	Target:	250K Paid	100 Clients
	Revenue:	~\$30M	\$30–40M
	Stats:	Proton AG \$70M revenue 2022	Expanding B2B contracts
Year 5	Target:	1M Paid	500 Clients
	Revenue:	~\$120M	\$150–200M
	Stats:	2–3% funnel conversion	Red Hat \$3B revenue 2018

Commercialization Summary

Revenue Trajectory (1-3y)

Pro USB

Y1: \$6M
Y2: \$30M
Y3: \$72-96M

Enterprise USB

Y1: \$3-4M
Y2: \$30-40M
Y3: \$150-200M

Encrypted USB

Y1: \$10-20M
Y2: \$25M
Y3: \$75M

Total ARR

Year 3: \$232-316M
(total annual reoccurring revenue)

— Beyond a hardware wallet: → Key protection is not enough. NØNOS secures the whole stack.

Industry Experts

Team & Advisors



Ek

Founder

Self-taught founder of NØNOS, creating the first Rust-based ZeroState OS with zk-proofs, sovereign mesh networking, and provable, portable post-identity applications.



Maxi

Growth Strategist

Growth strategist and Co-Founder of DGRS Labs, scaling AI applications with expertise in digital growth, user adoption, product scaling, and community engagement.



Pano

Creative Officer

Community leader, nonprofit executive, and Web3 innovator; bridges philanthropy and blockchain, leading youth development, capacity building, and global humanitarian initiatives.



Shek

Commercial Strategy & Partnerships Strategist and business development leader bridging institutional finance and Web3, driving adoption, fundraising, partnerships, and scaling decentralized privacy networks globally.



Bl4z3ng41n

Security & Platform Development

Technologist and builder specializing in cybersecurity, education, and advanced systems; develops AI-powered bots, decentralized apps, and fosters community collaboration and growth.



Hyp

Marketing & Strategy

Marketing strategist with a track record scaling companies to \$10M-\$60M; leverages Web3 and crypto expertise to drive branding, UX, SEO, user adoption, and global market expansion.



Darc

Web & UI Designer

Accomplished Web and UI Designer with experience leading crypto projects, combining creative direction and technical expertise to drive engagement, functionality, and growth.



Rustyx501

Software & Network Engineer

Building reliable kernels, distributed systems, and secure networking from the ground up. Focused on Rust-based performance, bare-metal development, and scalable infrastructure.



CryptoBobRoss

Crypto Veteran & Business Development Advisor

Crypto veteran, physician, and business development advisor, bridging blockchain, healthcare, and strategy to drive partnerships, scaling, and real-world impact.



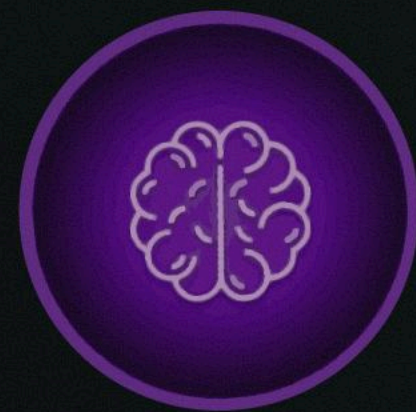
Daniel & Maxime

Strategic Advisors

Co-founders and key figures in the DePIN ecosystem; they scaled Hotspotty to 300,000 users, accelerated Helium network growth, and built DePINHub.io. Leveraging expertise in electrical engineering, hardware, data science, and enterprise software, they educate, advise, and connect the community while providing hands-on operational insights and structured learning pathways.

Industry Partners

Partners



PAAL



Hotspotty



Messier



DGRS



MAXKO



DeBros




IQ Wiki



Thank You

Join us in this journey to build the
world's first truly sovereign OS.

 nonos.systems

Secure by design. Private by default.