Rheo Neo-Sec “New-Security"

Neo-Sec: Proof-First Security for Critical Infrastructure

In an era where infrastructure is increasingly digitised, distributed, and exposed — **security begins with proof and culminates in detection**.

Neo-Sec (New Security) lays a new foundation for infrastructure-grade trust: a *proof-first* approach built for the physical-digital frontier.

Spun out of Rheo’s core verification layer — **Proof of Existence** — Neo-Sec delivers a tamper-evident, time-bound authentication layer for critical infrastructure. From green energy sites and data centres to supply chains and smart cities, it brings **programmable trust to the edge**.

While industries have advanced standards like KYC (Know Your Customer), KYB (Know Your Business), and KYT (Know Your Transactions/Technology), **Neo-Sec goes upstream — verifying the integrity of infrastructure itself**.

In today’s hybrid systems, where physical assets and digital control converge, one blind spot remains:

Who verified the infrastructure? Who owns the asset? Who activated it — when, and under what authority?

Neo-Sec answers these questions through a cryptographic lens. Whether for compliance, operational assurance, or automation, it enables partners to anchor trust where it matters most: **at the origin**.

Principles of Security:

1. Detection is reactive.

Most current cybersecurity models are built to **detect threats after they’ve already entered** a system or network. That’s like installing a fire alarm — helpful, but after the flames start.

2. Proof is proactive.

“Proof-first” approach means verifying **what, who, and when — before systems go live or data flows**. This is more like doing a fire safety inspection and certifying the building before occupancy. It’s upstream, preventive security.

3. Infrastructure is physical-digital.
When securing **critical infrastructure** (grids, smart meters, data centres), you need to prove that:

- The hardware is authentic
- The activation is authorised
- The system has not been tampered with

This can't be done with detection alone — it needs **verifiable, cryptographic proof** that precedes any data activity.

4. Proof is programmable trust.
For industries moving toward Automation, AI, and Web3 — **machine-level trust needs verifiable conditions**. Proof (like Rheo's "Proof of Existence") is how you build that logic layer.

Feature / Dimension	Rheo	Chainlink	Powerledger
Core Mission	Secure infrastructure & verify physical asset origin *before* data exists	Bring external data *into* smart contracts via oracles	Decentralised energy trading platform
Position in Data Lifecycle	Upstream – "Proof-before-oracle"	Midstream – Data ingestion and verification	Midstream – Energy data collection & tokenisation
Primary Focus	Trust layer for infrastructure integrity & real-world asset (RWA) tokenisation	Oracle network and data feeds	Peer-to-peer energy markets & renewables trading
Security Model	Zero Trust architecture, with edge attestation	Decentralised oracle nodes with crypto-economic incentives	IoT and event-based verification
Asset Onboarding	Verified physical assets → token issuance	External data (prices, APIs, weather) → smart contracts	IoT energy data → blockchain tokenisation

Token Utility	Infrastructure access, verification of staking, investment in tokenised RWAs	Payment for data feeds, node rewards	Energy trading, carbon credits
Commercial Model	B2B BaaS + VC-as-a-Platform	Developer middleware	Energy utilities, microgrids, and communities
Blockchain Ecosystem	Ethereum-first, expanding cross-chain	Multi-chain (Ethereum, BNB Chain, Arbitrum, others)	Ethereum & proprietary Powerledger blockchain
Target Sectors	Energy, compute, smart cities, supply chain, real-world infrastructure	Generalised smart contract use cases	Energy generation, trading, and community-driven utilities
Competitive Edge	**Security-first onboarding for RWAs** with market-ready investment infrastructure	Network effect in oracle data feeds	Early mover in green energy tokenisation

🔒 The Problem

Critical infrastructure — grids, meters, data centres, IoT — is the weakest link in global cyber defence.

Today's cybersecurity stops at data and identity. But who verifies the *infrastructure* itself?

🛡️ Our Solution

Neo-Sec applies **Proof-first Security**:

A tamper-evident, time-bound protocol that authenticates assets *before* they go online.

Powered by Rheo's **Proof of Existence**, Neo-Sec secures:

- ✅ Physical access and activation
- ✅ On-site asset verification
- ✅ Offline-to-on-chain trust bridging

💼 Our Commercialisation

Neo-Sec isn't just security infrastructure — it's also a gateway to **secure infrastructure investment**.
Through **Rheo's Venture Platform**, we are crafting a new category:

> **Security-led Infrastructure Capital** — where trusted assets meet trusted capital.

🔹 **Venture + Infrastructure**: Pairing high-assurance startups with verified real-world assets
🔹 **Blockchain as Security Product**: Proof-of-Existence becomes a standard for tradable, compliant infrastructure
🔹 **Investable Trust**: De-risked entry for capital markets, family offices, and industrial VCs

Neo-Sec powers a platform where **critical systems, emerging ventures, and capital markets converge — safely.**

🌍 Why Now

- **National Security:** Infrastructure is a new attack vector
- **Insurance Risk:** Cyber claims tied to unknown asset exposure
- **Regulatory Pressure:** NIS2, CISA, and critical infrastructure mandates
- **Web3 & AI:** Decentralisation needs verified physical anchors

---

⚙️ Unfair Advantage

- 🏗️ Commercial traction via Rheo in energy infra
- 🔗 Blockchain-native stack with enterprise reach
- 🌐 Real-world use cases: VPPs, data centres, edge devices

🤝 Coalition in Plan

Neo-Sec is building with:
• Cyber-aligned VCs
• Government advisors
• Industrial insurers

"Neo-Sec secures the last mile of trust — where humans, machines, and markets meet."