Getting Started

Copy

Introduction

Nerve Protocol is a privacy-native AI operating layer built on Trusted Execution Environments (TEEs), zero-knowledge attestations, and decentralized agent coordination. Every computation — inference, data retrieval, workflow execution — runs inside hardware-enforced enclaves. The host never sees plaintext. Not the cloud provider, not the inference node, not Nerve.

Nerve Protocol is currently in **public beta**, shipping with two purpose-built models:

Model	Class	Parameters	Context	Key Capability
Myelin	Edge / On-Device	4B	128K	Native audio + video, offline-capable, Apache 2.0
Soma	Flagship	32B	256K	Open weights, operator-defined policy, sealed TEE execution, Apache 2.0

CRYP2NOVA

What Nerve Protocol Enables

Operators use Nerve Protocol to run AI-driven workflows entirely within their own cryptographic boundary. The protocol handles:

Archived copy · cryp2nova.com

- **Encrypted session management** via the Nerve Console, a TEE-native interface where all state is sealed and only the operator holds the decryption keys.
- **Autonomous agent execution** inside attested enclaves, with policy capsules enforcing scope, retention, and intent at the hardware level.
- **Circuit-level data integration** across SaaS APIs (Uber, Amazon, Slack, Notion, Google Workspace), on-chain feeds, and air-gapped systems — without breaking the cryptographic perimeter.
- **Zero-knowledge receipts** for every job stage, enabling verifiable compliance without revealing payload content.

Core Security Guarantees

Nerve Protocol is built around a small set of non-negotiable properties:

Hardware isolation. AI inference, data retrieval, and agent execution occur inside Trusted Execution Environments. The host operating system and cloud provider cannot access enclave memory, even with root access to the underlying hardware.

Operator-held keys. Signing and decryption keys never leave the enclave. Even the Nerve orchestration layer cannot issue raw key material — it can only request capability proofs.

Verifiable execution. Every enclave used in a job publishes a remote attestation quote before and during execution. Compliance is proven via zero-knowledge receipts anchored to the Coordination Ledger, not via trust in Nerve as an intermediary.

Ephemeral compute. On job completion, enclave memory is wiped and session capsules dissolve. The ledger retains only attestation hashes — not payloads.

Archived copy · cryp2nova.com

Explore the Documentation

- Nerve Protocol Overview — architecture and core concepts
- Nerve Console — operator interface and session model
- How It Works — end-to-end execution flow
- Protocol Capabilities — full feature reference
- Access Tiers — plans and early access details
- Getting Started — first job walkthrough
- Integration Guide — connecting external systems
- Architecture — protocol layers and TEE design
- TEE Nodes — node verification and incentives
- $NRV Tokenomics — economic model and token mechanics

Next
Nerve Protocol Overview

Last updated 1 month ago

CRYP2NOVA

Archived copy · cryp2nova.com