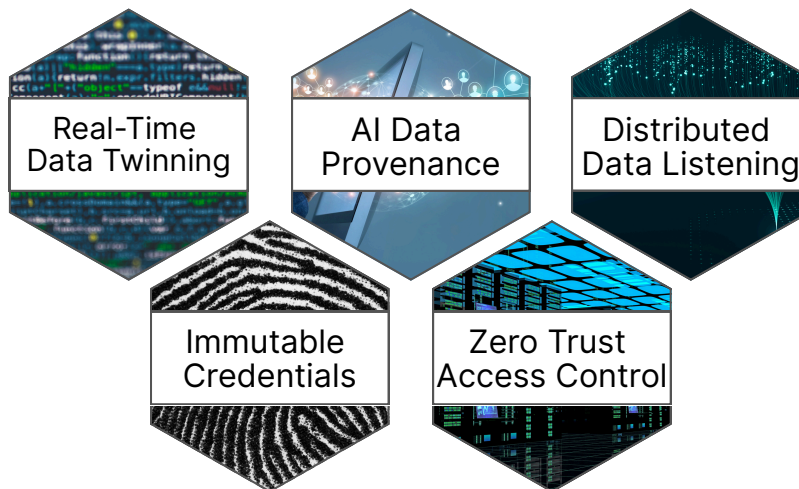


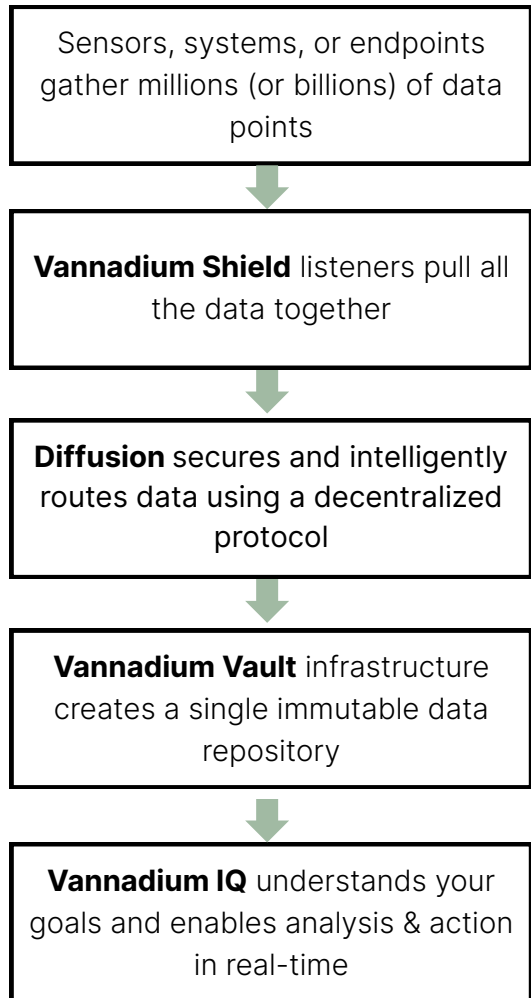
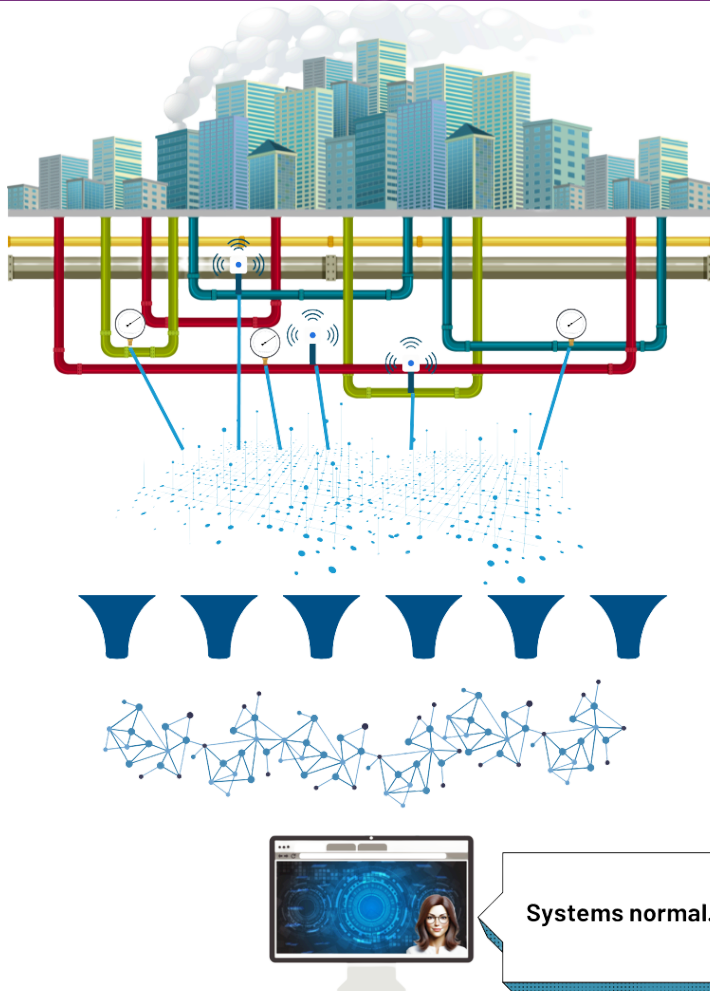
Real-Time Sovereign Data Infrastructure for a Post-Trust World

In an era where ransomware, data poisoning, and AI-driven threats are outpacing traditional defenses, Vannadium offers a new kind of resilience. We don't just secure the perimeter—we make the infrastructure itself sovereign, auditable, and instantly recoverable. Vannadium is the decentralized operating layer that enables real-time data control, automated trust, and system-wide situational awareness across critical industries.

Core Capabilities for Cybersecurity-Driven Organizations



- 1** **Ransomware-Resilient Architecture**
Real-time data twinning enables instant recovery from ransomware events with clean, immutable backups.
- 2** **Trustworthy AI Through Verifiable Data Sources**
Immutable provenance ensures AI systems operate on validated, transparent data.
- 3** **Secure, Distributed Data Listening at Scale**
Unify telemetry across fragmented systems, detect anomalies, and surface risks via our agentic AI layer.
- 4** **Credentialing and Access Verification**
On-chain digital credentials for workforce identity, equipment tracking, and access control.
- 5** **Decentralization for Compliance, Resilience, and Control**
Every access and action is policy-enforced, traceable, and logged—ideal for Zero Trust and regulated environments.



Where Vannadium fits in the stack

- Complements Zero Trust strategies with immutable audit and decentralized access enforcement
- Adds real-time visibility and trust to AI, credentialing, and secure data workflows
- Aligns with post-quantum goals—ensuring long-term data integrity and security
- Built for compliance: tamper-evident logs, federated data control, and audit readiness
- Functions as secure middleware with modular deployment across cloud, edge, or on-prem environments
- Enhances Data Loss Prevention (DLP) strategies with decentralized control and immutable recovery

Benefits & Business Value

- Resume operations in seconds post-ransomware
- Slash audit prep time from weeks to hours
- Reduce compliance costs and data risk exposure
- Improve AI reliability with trusted data pipelines
- Accelerate threat detection through unified, intelligent data listening
- Strengthen insider risk posture with traceable access and policy enforcement
- Enable secure collaboration across departments or partner networks