# Cilium Made eBPF the Network Data Plane. The Protocol Layer Carries No Governance.

by Nick Clark | Published March 28, 2026 | PDF

Cilium leverages eBPF to provide networking, security, and observability for Kubernetes and cloud-native environments. Its identity-aware enforcement, L7 policy support, transparent encryption, and Hubble observability represent the state of the art in cloud-native networking. But Cilium's intelligence lives in the enforcement layer. The traffic being enforced upon carries standard IP packets with no governance semantics. Cilium inspects and decides from outside the protocol. The gap is between intelligent enforcement infrastructure and protocol semantics where governance is intrinsic to the content.

---

Cilium's use of eBPF for programmable kernel-level networking is technically impressive. The combination of identity-aware enforcement, Hubble flow observability, and ClusterMesh multi-cluster connectivity addresses real operational challenges. The gap described here is about what the protocol carries, not about what eBPF can inspect.

## Identity-aware enforcement on identity-unaware traffic

Cilium assigns cryptographic identities to workloads based on Kubernetes labels. These identities are maintained in Cilium's own identity management system and mapped to eBPF programs that enforce policies. The enforcement is identity-aware. But the packets themselves are standard IP packets. They carry no identity information. Cilium identifies them by their source and context, not by what the packets themselves declare.

If a packet appears from an unexpected source or if the identity mapping is stale, the enforcement system must handle the mismatch. The traffic cannot self-identify. It depends on the infrastructure to identify it.

## L7 inspection as protocol intrusion

Cilium can enforce policies at L7, inspecting HTTP headers, gRPC methods, and DNS queries. This provides fine-grained control. But L7 inspection means the enforcement layer must parse application protocols to extract governance-relevant information. The governance information is not in the protocol's native structure; it must be extracted from application-level content.

Each new application protocol that needs governance enforcement requires new parsing logic in Cilium. The governance capability grows with the enforcement layer, not with the protocol.

## What memory-native protocol semantics provide

A memory-native protocol would embed governance semantics at the protocol level, eliminating the need for external identity mapping and L7 parsing. Each packet would carry its own trust scope, governance constraints, and routing authority as protocol-native fields. Cilium's eBPF programs could enforce these protocol-native governance fields at kernel speed without parsing application-layer content.

The enforcement would shift from inferring governance from infrastructure metadata and application-layer inspection to validating governance fields that the protocol itself carries.

## The remaining gap

Cilium brought programmable, identity-aware networking to Kubernetes through eBPF. The remaining gap is in the protocol layer: whether governance can be a protocol-native property rather than an inference made by the enforcement infrastructure.

Memory-Native Protocol All 21 steps →

Authority intrinsic to the object. Routing by semantic properties.

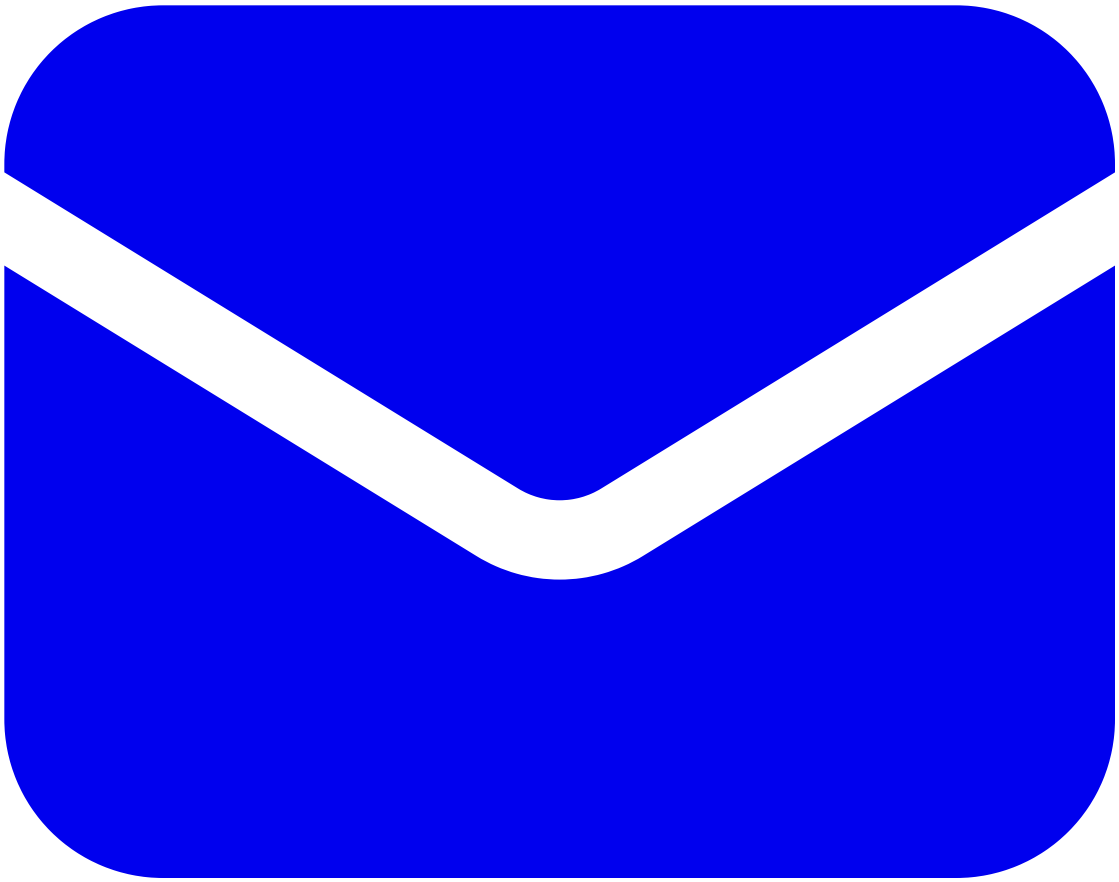
Patent
US 19/366,760 · filed
Primary Technical Disclosure
○ Memory-Native Networking: A Cognition-Compatible Protocol Substrate
Secondary Technical
○ Protocol-Native Carriers: Agents as the Fundamental Unit of Transmission○ Dynamic Routing Protocol: Memory-Aware Path Selection for Semantic Agents○ Trust-Weighted Route Scoring: Dynamic Path Selection Through Policy-Defined Trust Thresholds○ Network Health Monitoring System: Signed Health Agents as Distributed Operational Telemetry○ Health Agents as Semantic Objects: Operational Metrics That Route Like Any Other Agent○ Dynamic Indexing Protocol: Entropy-Driven Restructuring of Semantic Flows○ Soft-Index Anchors: Ephemeral Index Points Inferred From Agent Lineage○ Adaptive Consensus Protocol: Memory-Native Quorum Without Fixed Validator Sets○ Trust-Weighted Voting in ACP: Domain-Scoped Votes Accumulated Against Agent Memory○ Dynamic Alias Resolution: Zone-Local Semantic Aliases Resolved Through Transport Headers○ Horizontally Composable Protocol Stack: Independent Layers Operating in Parallel○ Transport-Layer Agnosticism: One Protocol Stack Above Any Carrier○ Federated Semantic Zone Deployment: Heterogeneous Nodes Coordinating Across Trust Boundaries○ Health-Triggered Quorum Adjustment: Dynamic Thresholds From Network Stability Signals
Applications (General)
○ Edge Computing Without Central Routing Authority○ IoT Device Mesh Governance at Scale○ Vehicle-to-Vehicle Communication With Intrinsic Governance○ Military Mesh Networks Without Central Routing Authority○ Smart City Infrastructure With Self-Governing Transport○ Satellite Communication With Delay-Tolerant Governance○ Industrial IoT Protocols With Embedded Authority○ Healthcare Device Mesh Networking
Applications (Specific)
○ Starlink Built a Satellite Mesh. The Routing Authority Is Still Terrestrial.○ Zigbee Built a Mesh Protocol for IoT. The Messages It Carries Have No Memory.○ Matter Unified Smart Home Devices. The Protocol Still Separates Data From Authority.○ Helium Decentralized Wireless Coverage. The Protocol That Uses It Did Not Follow.○ LoRaWAN Solved Long-Range IoT. The Messages Are Still Passive Payloads.○ Tailscale Made WireGuard Usable. The Coordination Server Still Holds the Authority.○ QUIC Modernized Transport. The Protocol Carries No Semantic Authority.○ MQTT Connected Billions of IoT Devices. The Broker Still Holds the Authority.○ CoAP Brought REST to Constrained Devices. The Protocol Carries No Governance Semantics.○ gRPC Made Service Communication Type-Safe. The Protocol Carries No Trust Semantics.○ ZeroMQ Eliminated the Broker. Routing Authority Still Lives in Application Code.○ WireGuard Simplified VPN Tunnels. The Protocol Has No Semantic Routing Layer.○ Nebula Built Overlay Mesh Networks. The Certificate Authority Is Still Central.○ Calico Enforces Network Policy at the Kernel Level. Policy Authority Is Still External.● Cilium Made eBPF the Network Data Plane. The Protocol Layer Carries No Governance.○ Weave Net Built a Virtual Network for Containers. The Protocol Carries No Semantic Authority.
Memory-Native Protocol overview →
AQ
deterministic
autonomy

Legal

Subject to one or more pending U.S. and international patent applications, see Patents for the current list and status. No license, express or implied, is granted. Any use requires a separate written agreement—see Licensing. Patent applications referenced on this site are pending. Claim scope, if any, is subject to examination and may issue in altered form or not at all. See Legal for terms and conditions.



Last updated: 2026-03-03




- 
- nick@qu3ry.net
- 72 28 14 36 01

Invented by Nick Clark | Founding Investors: Devin Wilkie