Health Monitoring: Unified Governance and Supply-Chain Composite

by Nick Clark | Published April 25, 2026

Three Independent Disciplines Solving Adjacent Pieces of One Problem

Zero-trust device management (Microsoft Defender, CrowdStrike, Armis, Claroty) authenticates device identity through credential checks. The discipline is mature but operates on present-state credentials without continuous behavioral baseline.

Supply-chain attestation (Sigstore, in-toto, Chainguard, software bill-of-materials) traces software components back to their sources. The discipline produces tamper-evident provenance but operates on artifacts rather than running devices.

Trust-slope anomaly detection (UEBA, Endpoint Detection and Response) flags behavioral departures from device baselines. The discipline catches behavioral anomalies but lacks the cryptographic provenance and governance-chain context that authoritative response requires.

Each discipline does its own piece. None integrate. A regulated fleet operator running compliance under UNECE R155, FDA PMA, EU MDR, or NIS2 needs all three views composed into a single auditable assessment, and currently has to integrate them ad hoc.

1. The Primitive: Composite Fleet-Health Observation

The health monitoring primitive produces a single composite credentialed observation per device, integrating: governance-chain credential status (current credential authority, credential continuity over time, revocation status, trust-slope behavioral baseline), supply-chain provenance status (silicon PUF challenge-response liveness, SBOM verification, seal-tamper status), and operational context (capability envelope, mission policy, regulatory framework).

The composite observation is signed by a credentialed health authority — possibly the device owner, possibly a third-party compliance attester, possibly a regulator. The signature attests to the authority's evaluation of the constituent observations against the policy under which the device operates.

Health observations propagate through the mesh like any other governed observation. Other systems (peer devices, infrastructure agents, regulators, insurers) consume the observation through composite admissibility, with the health attestation modulating evidential weight, capability admission, and operational authority.

2. Governance-Chain Integrity Sub-Components

The governance-chain integrity component continuously evaluates: credential freshness (the device's current credential is not expired, revoked, or superseded), credential continuity (the device's credential history shows an unbroken trust-slope chain back to its issuance), revocation propagation (the device is responsive to revocation observations the governing authority has issued), and behavioral consistency (the device's recent observations are consistent with its long-term behavioral baseline under trust-slope analysis).

Each sub-component produces its own credentialed observation that the composite health attestation references. Failures are recorded with reasons; passes are recorded

with the supporting observations. Lineage admits forensic reconstruction of how a health attestation was produced.

The governance-chain integrity view is forward-looking: it assesses whether the device is currently and continuously the trustworthy entity its credential claims, rather than assessing whether the credential was valid at issuance.

3. Supply-Chain Provenance Sub-Components

The supply-chain provenance component evaluates the device's physical and software lineage. Silicon PUF challenge-response provides tamper-evident proof that the device contains the specific silicon it was credentialed with at manufacture (an attacker substituting hardware fails the PUF challenge). SBOM attestation verifies that the running firmware matches the declared software bill-of-materials, signed by the build authority.

Tamper-evident seal monitoring (where applicable) provides physical attestation that the device's enclosure has not been opened since credentialing. The seal observation is signed by the most recent inspection authority (manufacturer at packaging, deployer at installation, periodic auditor in operation).

Supply-chain provenance is backward-looking: it assesses whether the device's current state derives consistently from its credentialed origin. Combined with governance-chain integrity (forward-looking), the composite covers the full trust-history.

4. Composite Fleet-Health Across Cross-Domain Aggregation

Single-device health is a starting point. Real regulated fleets need composite health across thousands or millions of devices, with cross-domain aggregation that respects

authority boundaries: an OEM sees its own deployed devices; a fleet operator sees its own operating fleet; a regulator sees attestations across regulated populations.

Aggregation is governance-credentialed: an aggregator (OEM, fleet operator, regulator) consumes credentialed device-level observations within its scope and produces credentialed aggregate observations. The aggregator's credential and the aggregation policy are both audit-grade.

Cross-domain aggregation handles cases like UNECE R155 cybersecurity reporting (where a vehicle OEM aggregates across deployed vehicles for type-approval reporting) and FDA post-market surveillance (where a medical device manufacturer aggregates across deployed devices for adverse-event reporting). The mechanism is the same; the configurations differ.

5. Zero-Trust Integration Without Reimplementation

Zero-trust device management products consume the composite health observation as a credentialed input. A Microsoft Defender or CrowdStrike policy can be configured to allow an action only if the composite health observation satisfies a threshold; the integration is policy-level rather than architectural.

This is decisive for adoption. Zero-trust products have made significant deployment progress and operators are not going to replace them. The governed primitive provides the unified observation those products are missing; the products consume it without abandoning their existing investment.

The same is true for security operations centers (SOC), security information and event management (SIEM), and endpoint detection and response (EDR) platforms. The composite health observation is a structured input that integrates into existing toolchains.

6. Compliance-Driven Adoption

Regulatory compliance is the demand driver. UNECE R155 (vehicle cybersecurity, mandatory in the EU and adopted by reference in many other jurisdictions), FDA PMA post-market surveillance, EU MDR for medical devices, NIS2 for critical infrastructure, and similar regulations are converging on requirements that map directly to the composite health observation.

The regulations effectively require what the primitive produces: continuous device-health attestation with cryptographic provenance, supporting forensic reconstruction, with audit-grade aggregation across regulated fleets. Regulators are arriving at the same architectural endpoint independently of industry.

The patent reaches every regulated-fleet operator who must produce composite health attestation for compliance. Adoption is not driven by operator preference but by regulatory mandate, with the primitive providing the most structurally efficient implementation path.

7. What This Is Not

This is not zero-trust device management. ZTDM is a single component (governance-chain integrity); the governed primitive composes it with supply-chain provenance and trust-slope behavioral analysis.

This is not Sigstore or in-toto attestation. Those are supply-chain provenance components; the governed primitive composes them with governance-chain integrity for running-device assessment.

This is not UEBA / EDR. Those are behavioral-anomaly components; the governed primitive composes them with cryptographic provenance for authoritative response.

Conclusion

Health monitoring unifies three disciplines — zero-trust device management, supply-chain provenance, and trust-slope behavioral analysis — into a single composite credentialed observation that regulated-fleet operators can produce, audit, and report. Compliance regulations across vehicles, medical devices, and critical infrastructure are converging on the requirement.

Disclosed under USPTO provisional 64/049,409, the primitive integrates with mesh-distributed firmware updates (Article 1), confidence-governed actuation (Article 2), and the broader governance chain umbrella (Article 15).