Zero-Trust Device Management

by Nick Clark | Published April 25, 2026

What It Specifies

The architecture admits unit operations only against current health attestation. Stale attestation, failed verification, or revoked admissibility all produce structural exclusion until renewed attestation.

Zero-trust admissibility is governance-credentialed. The admissibility authority, the requirements, and the resulting admissibility states all enter lineage; downstream operations admit only against current admissibility.

Why It Matters Structurally

Trust-by-default device management produces structural risk. Compromised, malfunctioning, or revoked units may continue operating until detected; the architecture must require continuous attestation structurally.

Zero-trust management produces structural defense. The architecture excludes non-attesting units; compromised units lose admissibility; operations continue only against currently-attesting units.

How It Composes With Mesh Operation

The architecture defines the attestation requirements, the admissibility-lapse handling, and the renewal protocol. Implementations apply the architecture; device management operations proceed within the framework.

Zero-trust composes with other features. Cross-mesh zero-trust federation, byzantine-robust admissibility evaluation, and dispute mechanism for admissibility disputes all build on the zero-trust primitive.

What This Enables

Defense device management gains structurally-supported zero-trust. Civilian critical-infrastructure device management gains the same.

The architecture also supports zero-trust evolution. As zero-trust standards mature, attestation protocols update through governance procedures.