Governance-by-Infra-Design

Subject: Infra AI Traceability & Immutable Audit Trails

1. Summary

As defense sectors adopt autonomous AI, a compliance gap emerges due to the inability to explain AI decisions. This whitepaper proposes "Governance-by-Design," embedding "Audit-as-a-Service" into the infrastructure kernel. It ensures that every AI decision is cryptographically signed, logged, and immutable, ensuring 100% pass rates on safety audits.

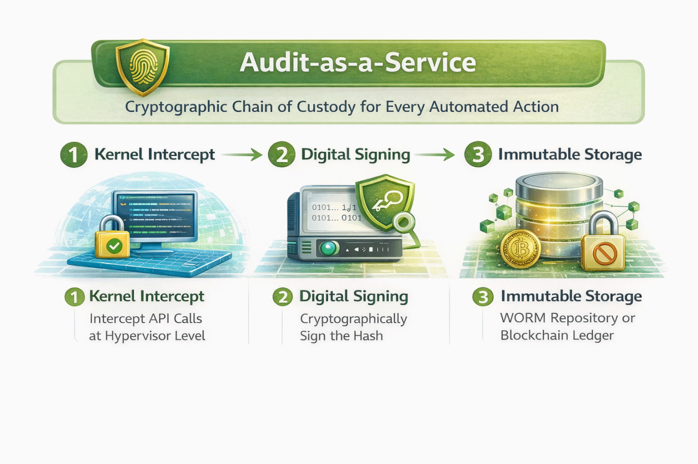
2. The Infrastructure Problem: The "Black Box" of Autonomy

Defense and high-security sectors operate under strict Rules of Engagement (ROE) and safety protocols. However, modern Deep Learning models function as "Black Boxes."

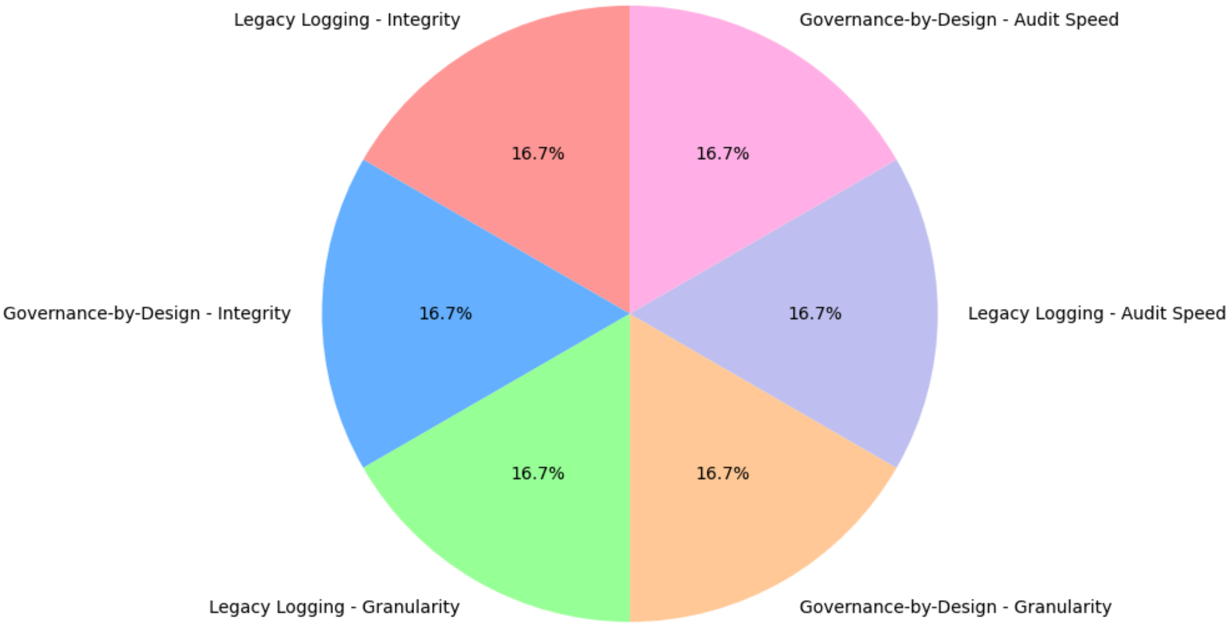
When an automated system executes a command (e.g., re-routing a drone or flagging a target), the internal logic is often transient and lost. This creates two major risks:

- **Compliance Failure:** Without a verifiable log of the *decision path*, systems cannot pass standard safety audits (ISO/IEC standards).
- **Tampering Risk:** Standard log files are mutable. In the event of an incident, root access holders could theoretically alter logs to cover up errors or malicious injections.

3. The Engineering Solution: Kernel-Level



5. Strategic Benefits



Comparison: Legacy Logging vs Governance-by-Design