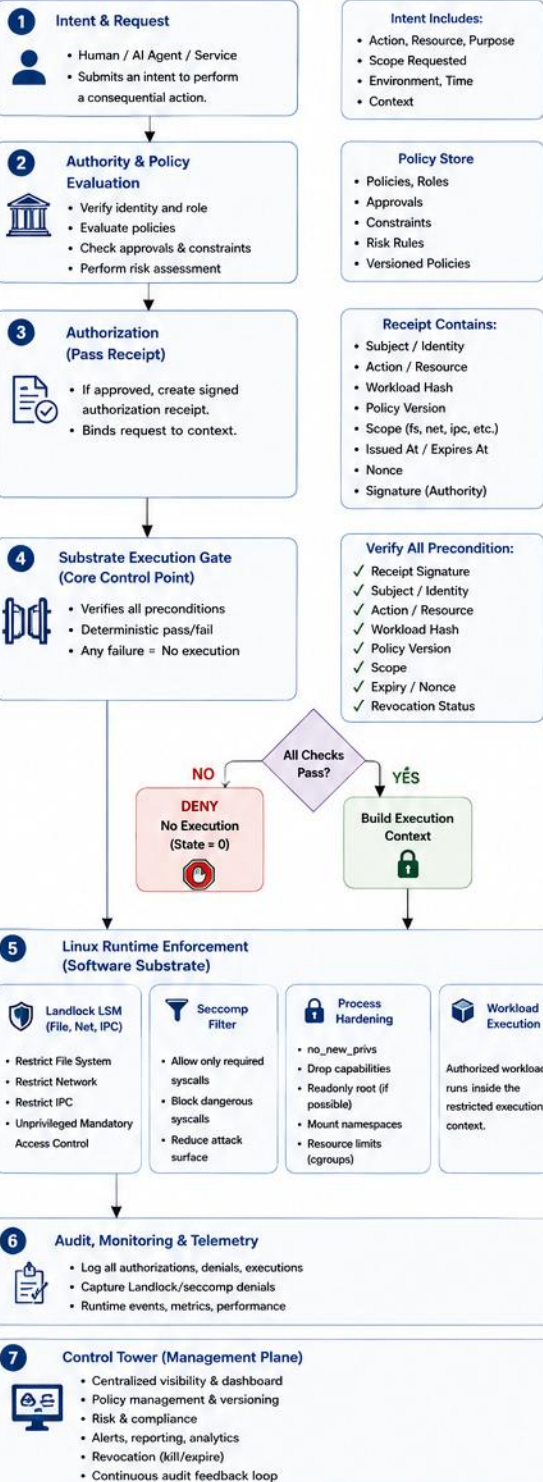


BARE METAL / SUBSTRATE SECURITY ARCHITECTURE

End-to-End Flow: Without Hardware vs With Hardware (Hardware-Enhanced)

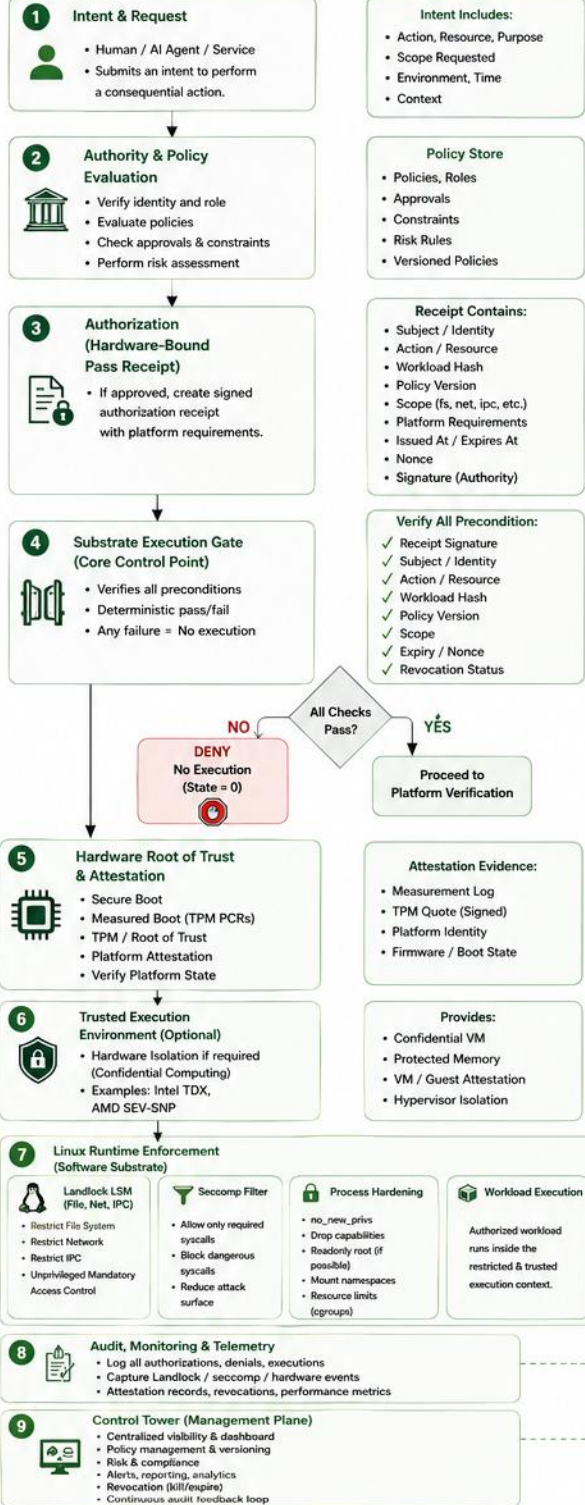
A. WITHOUT HARDWARE (Software-Only)

Linux Substrate Enforcement with Landlock



B. WITH HARDWARE (Hardware-Enhanced)

Hardware Root of Trust + Attestation + Confidential Execution (Optional)



HOW THE TWO ARCHITECTURES DIFFER

Aspect	A. Without Hardware (Software-Only)	B. With Hardware (Hardware-Enhanced)
Platform Trust	Relies on OS & policies	Hardware Root of Trust (TPM, Secure Boot, Measured Boot)
Isolation Strength	Process-level restriction only	Stronger (TEE / confidential VM isolation)
Attestation	Not available	Hardware-backed attestation available
Trust Boundary	OS / Kernel boundary	Hardware-rooted trust boundary
Use Cases	General workloads, standard cloud/edge	High assurance, sensitive workloads, regulated environments
Complexity	Lower (easy to deploy)	Higher (requires hardware support)

KEY BENEFITS (BOTH ARCHITECTURES)

- ✓ Quiescent by Default (no valid auth = no execution)
- ✓ Deterministic Pass / Fail (no probabilistic detection)
- ✓ Zero-Drift (bound to policy, workload, platform)
- ✓ Least Privilege by Design
- ✓ Immutable Audit & Forensic Readiness
- ✓ Reduces Drift Tax & Operational Waste

LEGEND (Flow Symbols)

→ Normal Flow - - - - Audit / Feedback Loop ◇ Decision Point □ Process / Activity [] Data Store / Policy Store 🔒 Secure / Protected 📄 Receipt / Data 🏠 Hardware / Root of Trust 🏠 Execution / Workload