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

1 Intent & Request

- Human / AI Agent / Service
- Submits an intent to perform a consequential action.

Intent Includes:
- Action, Resource, Purpose
- Scope Requested
- Environment, Time
- Context

2 Authority & Policy Evaluation

- Verify identity and role
- Evaluate policies
- Check approvals & constraints
- Perform risk assessment

Policy Store
- Policies, Roles
- Approvals
- Constraints
- Risk Rules
- Versioned Policies

3 Authorization (Pass Receipt)

- If approved, create signed authorization receipt.
- Binds request to context.

Receipt Contains:
- Subject / Identity
- Action / Resource
- Workload Hash
- Policy Version
- Scope (fs, net, ipc, etc.)
- Issued At / Expires At
- Nonce
- Signature (Authority)

4 Substrate Execution Gate (Core Control Point)

- Verifies all preconditions
- Deterministic pass/fail
- Any failure = No execution

Verify All Precondition:
- ✓ Receipt Signature
- ✓ Subject / Identity
- ✓ Action / Resource
- ✓ Workload Hash
- ✓ Policy Version
- ✓ Scope
- ✓ Expiry / Nonce
- ✓ Revocation Status

All Checks Pass?

NO → **DENY** No Execution (State = 0)

YES → **Build Execution Context**

5 Linux Runtime Enforcement (Software Substrate)

Landlock LSM (File, Net, IPC)
- Restrict File System
- Restrict Network
- Restrict IPC
- Unprivileged Mandatory Access Control

Seccomp Filter
- Allow only required syscalls
- Block dangerous syscalls
- Reduce attack surface

Process Hardening
- no_new_privs
- Drop capabilities
- Readonly root (if possible)
- Mount namespaces
- Resource limits (cgroups)

Workload Execution

Authorized workload runs inside the restricted execution context.

6 Audit, Monitoring & Telemetry

- Log all authorizations, denials, executions
- Capture Landlock/seccomp denials
- Runtime events, metrics, performance

7 Control Tower (Management Plane)

- Centralized visibility & dashboard
- Policy management & versioning
- Risk & compliance
- Alerts, reporting, analytics
- Revocation (kill/expire)
- Continuous audit feedback loop

B. WITH HARDWARE (Hardware-Enhanced)

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

1 Intent & Request

- Human / AI Agent / Service
- Submits an intent to perform a consequential action.

Intent Includes:
- Action, Resource, Purpose
- Scope Requested
- Environment, Time
- Context

2 Authority & Policy Evaluation

- Verify identity and role
- Evaluate policies
- Check approvals & constraints
- Perform risk assessment

Policy Store
- Policies, Roles
- Approvals
- Constraints
- Risk Rules
- Versioned Policies

3 Authorization (Hardware-Bound Pass Receipt)

- If approved, create signed authorization receipt with platform requirements.

Receipt Contains:
- Subject / Identity
- Action / Resource
- Workload Hash
- Policy Version
- Scope (fs, net, ipc, etc.)
- Platform Requirements
- Issued At / Expires At
- Nonce
- Signature (Authority)

4 Substrate Execution Gate (Core Control Point)

- Verifies all preconditions
- Deterministic pass/fail
- Any failure = No execution

Verify All Precondition:
- ✓ Receipt Signature
- ✓ Subject / Identity
- ✓ Action / Resource
- ✓ Workload Hash
- ✓ Policy Version
- ✓ Scope
- ✓ Expiry / Nonce
- ✓ Revocation Status

All Checks Pass?

NO → **DENY** No Execution (State = 0)

YES → **Proceed to Platform Verification**

5 Hardware Root of Trust & Attestation

- Secure Boot
- Measured Boot (TPM PCRs)
- TPM / Root of Trust
- Platform Attestation
- Verify Platform State

Attestation Evidence:
- Measurement Log
- TPM Quote (Signed)
- Platform Identity
- Firmware / Boot State

6 Trusted Execution Environment (Optional)

- Hardware Isolation if required (Confidential Computing)
- Examples: Intel TDX, AMD SEV-SNP

Provides:
- Confidential VM
- Protected Memory
- VM / Guest Attestation
- Hypervisor Isolation

7 Linux Runtime Enforcement (Software Substrate)

Landlock LSM (File, Net, IPC)
- Restrict File System
- Restrict Network
- Restrict IPC
- Unprivileged Mandatory Access Control

Seccomp Filter
- Allow only required syscalls
- Block dangerous syscalls
- Reduce attack surface

Process Hardening
- no_new_privs
- Drop capabilities
- Readonly root (if possible)
- Mount namespaces
- Resource limits (cgroups)

Workload Execution

Authorized workload runs inside the restricted & trusted execution context.

8 Audit, Monitoring & Telemetry

- Log all authorizations, denials, executions
- Capture Landlock / seccomp / hardware events
- Attestation records, revocations, performance metrics

9 Control Tower (Management Plane)

- Centralized visibility & dashboard
- Policy management & versioning
- Risk & compliance
- Alerts, reporting, analytics
- Revocation (kill/expire)
- Continuous audit feedback loop

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