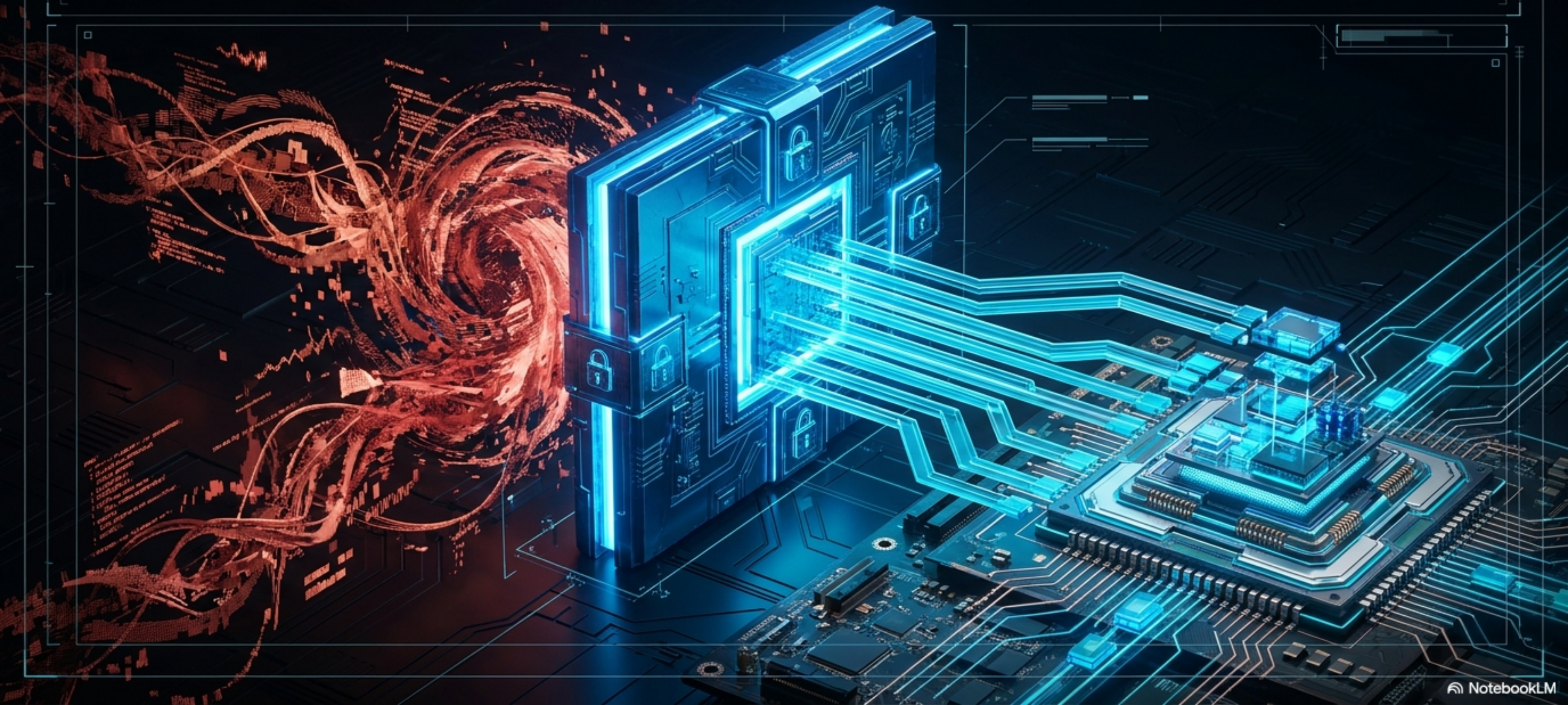


AXIS SWGI™: Govern Before Execution

Deterministic Execution Governance for Sovereign AI, Cloud, and Mission-Critical Infrastructure.



THE CRISIS OF REACTIVE INFRASTRUCTURE SECURITY

As AI workloads become autonomous and data centers hit critical power limits, traditional OS-level security fails. Relying on post-execution monitoring means the infrastructure has already been compromised and expensive compute has already been consumed.

THE PROBABILISTIC REALITY



THE THERMODYNAMIC COST



Security: Vulnerable to autonomous AI actions executing before human intervention.



Compute: Heavy infrastructure drag and unnecessary token consumption.



Compliance: Interpretive, post-event logs rather than absolute mathematical proof.

FROM PROBABILISTIC OBSERVATION TO DETERMINISTIC GOVERNANCE

True Zero Trust must extend past the network perimeter and directly into the micro-operations of the workload execution layer.

THE TRADITIONAL PARADIGM

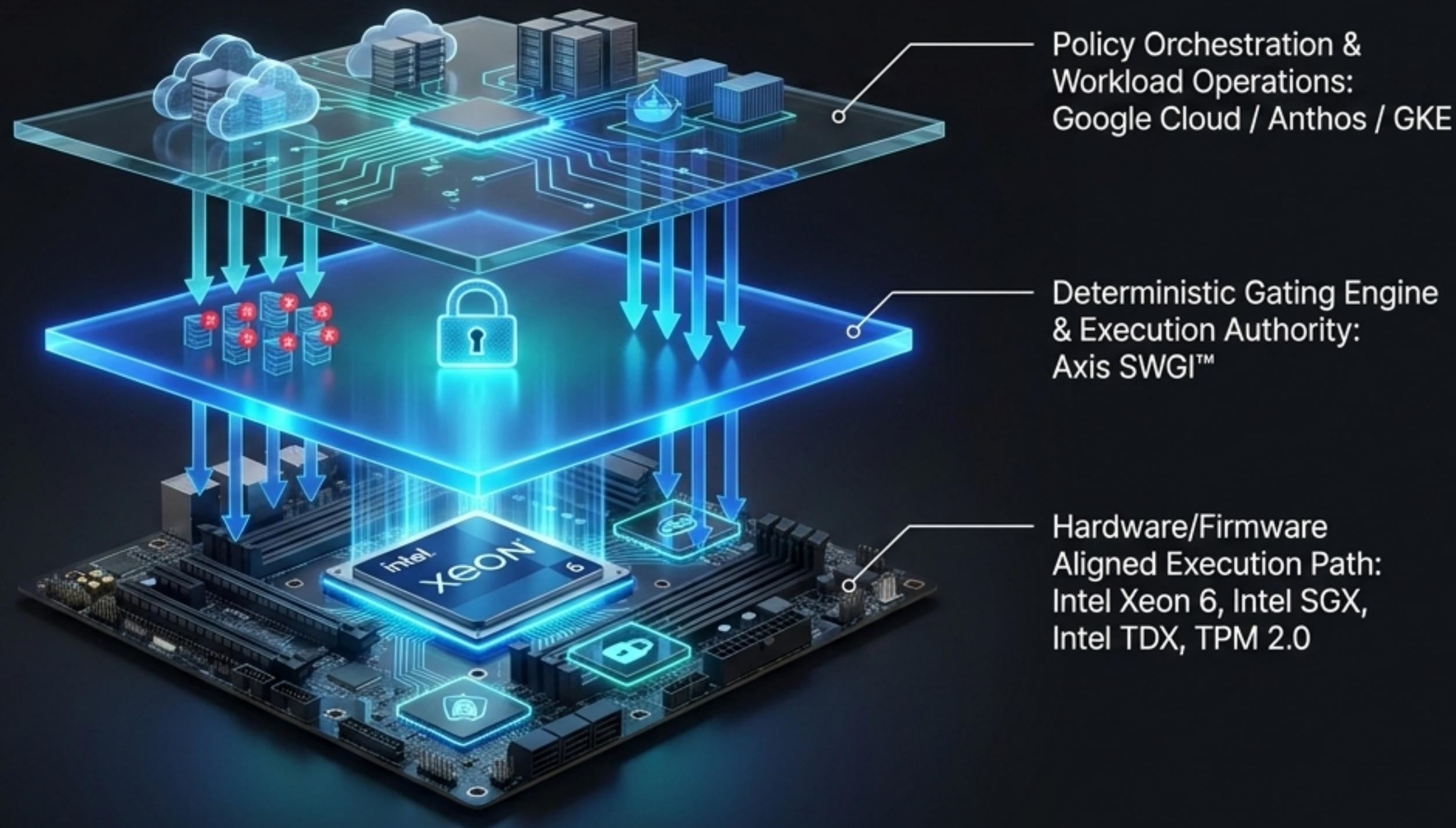
Mechanism	Detect -> Log -> Remediate
Timing	Post-execution (Reactive)
Latency	High (Human or asynchronous loop)
Compliance	Reconstructed after the fact from fragmented telemetry
Compute Waste	High (Resources are consumed while the system decides if the action was safe)

THE SWGI™ PARADIGM

Mechanism	Authorize -> Execute -> Prove
Timing	Pre-execution (Proactive)
Latency	Sub-millisecond (~0.25ms) hardware-triggered
Compliance	Immutable, hardware-anchored cryptographic receipts generated at runtime
Compute Waste	Zero at the unauthorized execution layer (Blocked before clock advancement)

The Execution Authority Layer

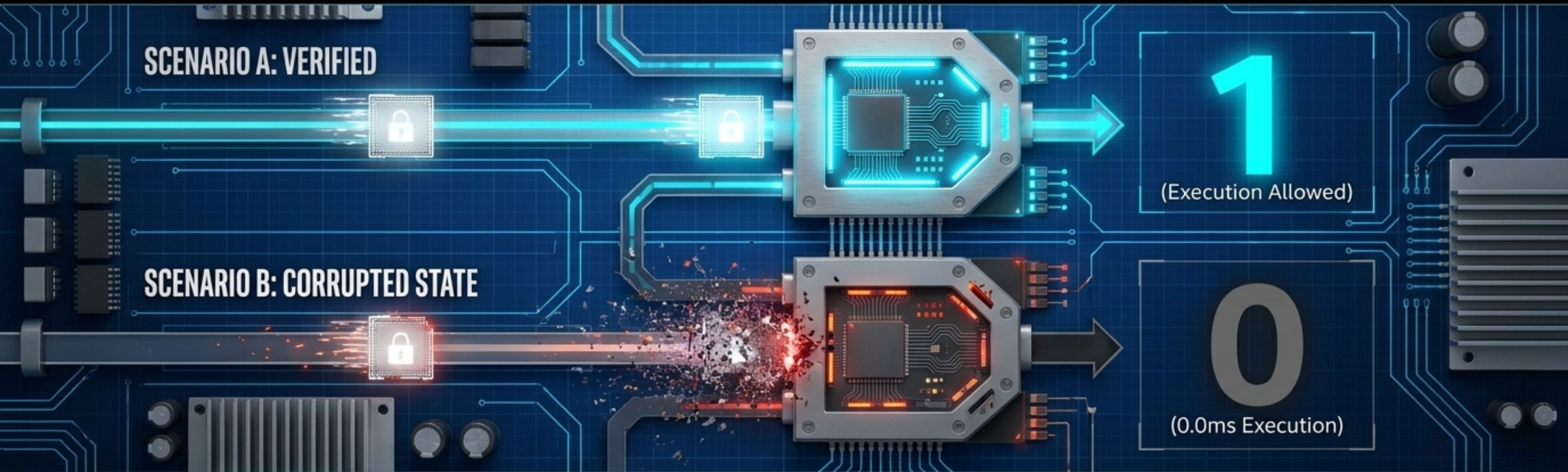
SWGITM does not replace Google Cloud or Intel; it acts as the Immutable Handshake between them.
If a workload lacks verified authority, it never touches the silicon.



INTENT-AWARE ARCHITECTURE: THE MATH OF TRUST

Execution is a binary outcome: $g\pi \in \{0, 1\}$. There is no probabilistic guessing and no partial credit.

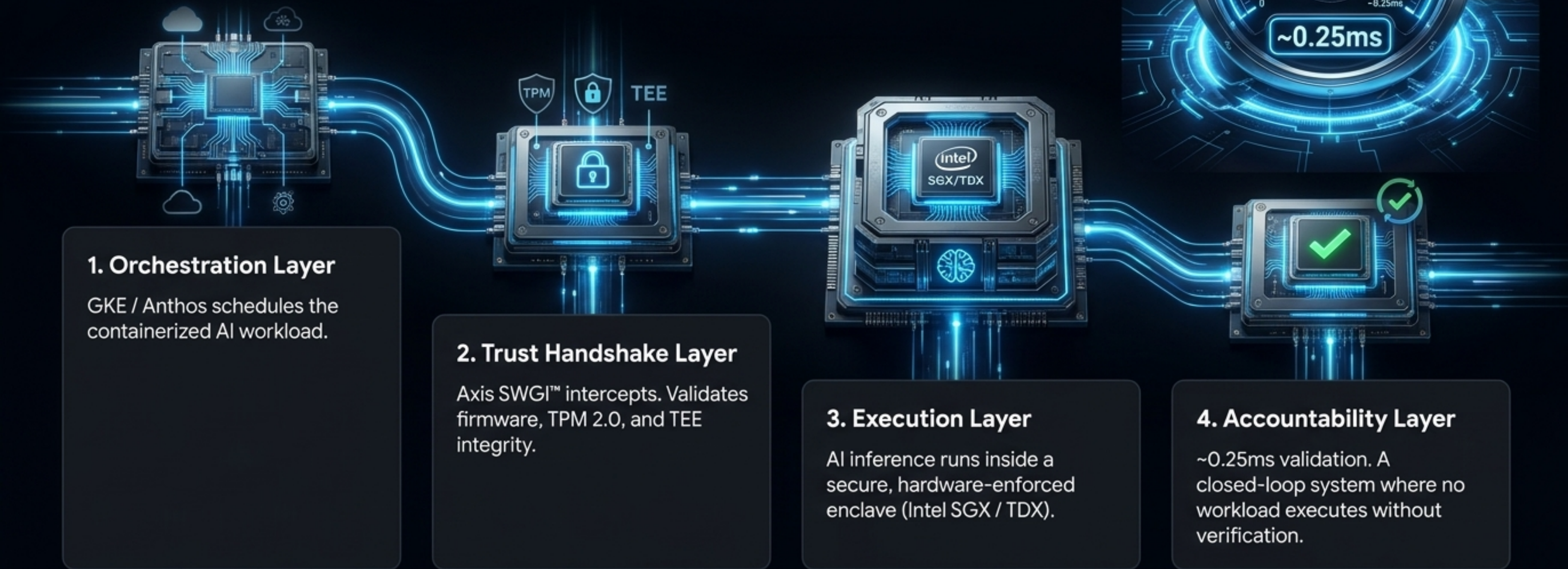
EXECUTE = F(INTENT, STATE, POLICY, AUTHORITY, PROOF)



SWGf enforces absolute mathematical truth. If a specific mission target is not 100% verified, the gate stays shut.
We isolate failure at the atomic level without stopping the healthy data.

The ~0.25ms Deterministic Pipeline

Enforcing Zero Trust at the micro-operation level with near-zero latency.



Cryptographic Trust Receipts™: The Ultimate Evidence

Moving from interpreted logs to absolute science. Every governed execution produces an immutable, hardware-anchored SHA-256 receipt.



Identity: Who authorized the execution?



Policy: Which governance rule permitted this?



Intent: What was the workload?



State: Was the hardware (TPM/Firmware) verified?



Time: When did execution occur?

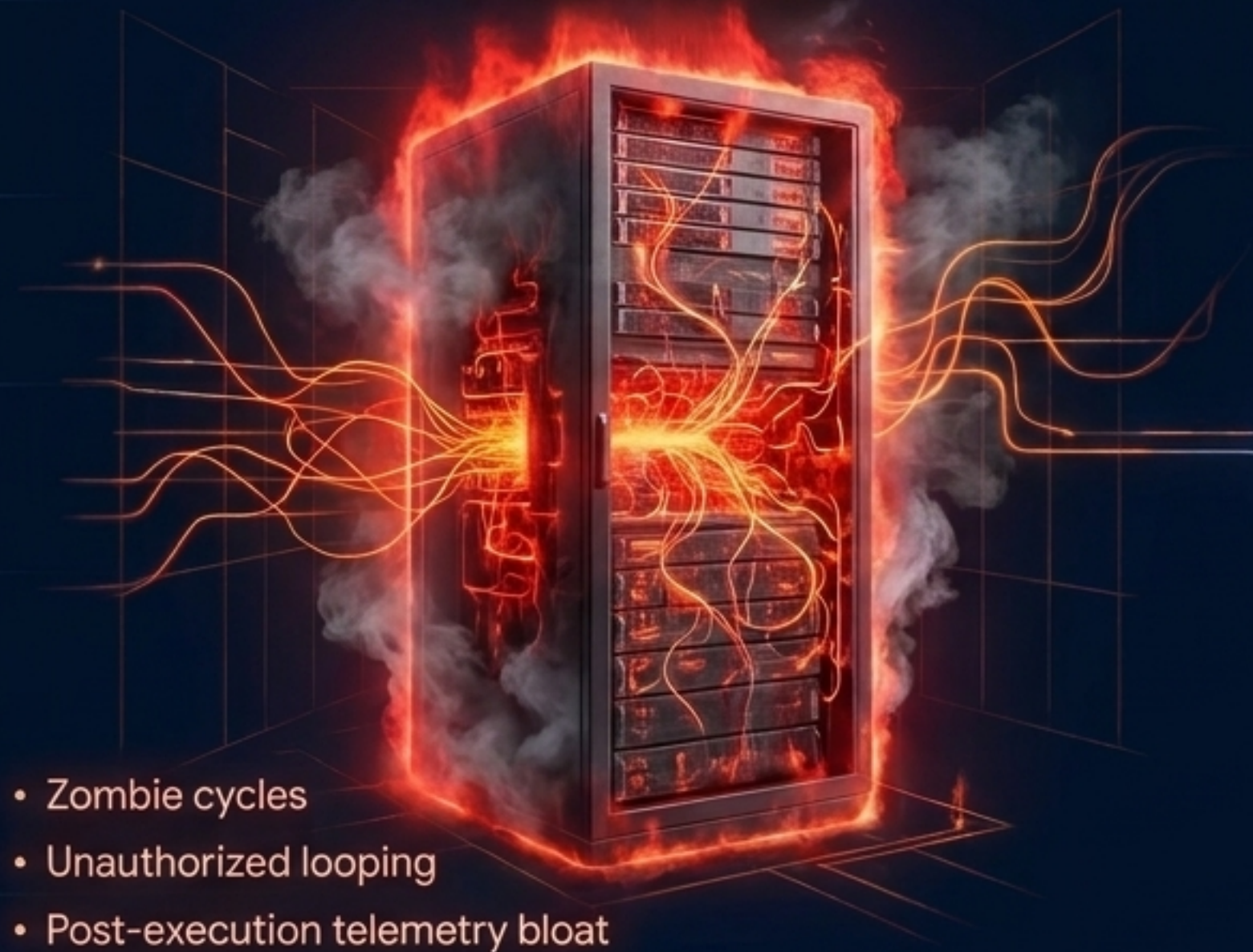
SHA-256
Signature



Green Compute By Design: The Hidden Dividend

By intercepting unauthorized, idle, or malicious workloads before they execute, SWGI reclaims up to 40-80% of wasted Ghost Compute.

Traditional Rack



- Zombie cycles
- Unauthorized looping
- Post-execution telemetry bloat

SWGI Governed Rack

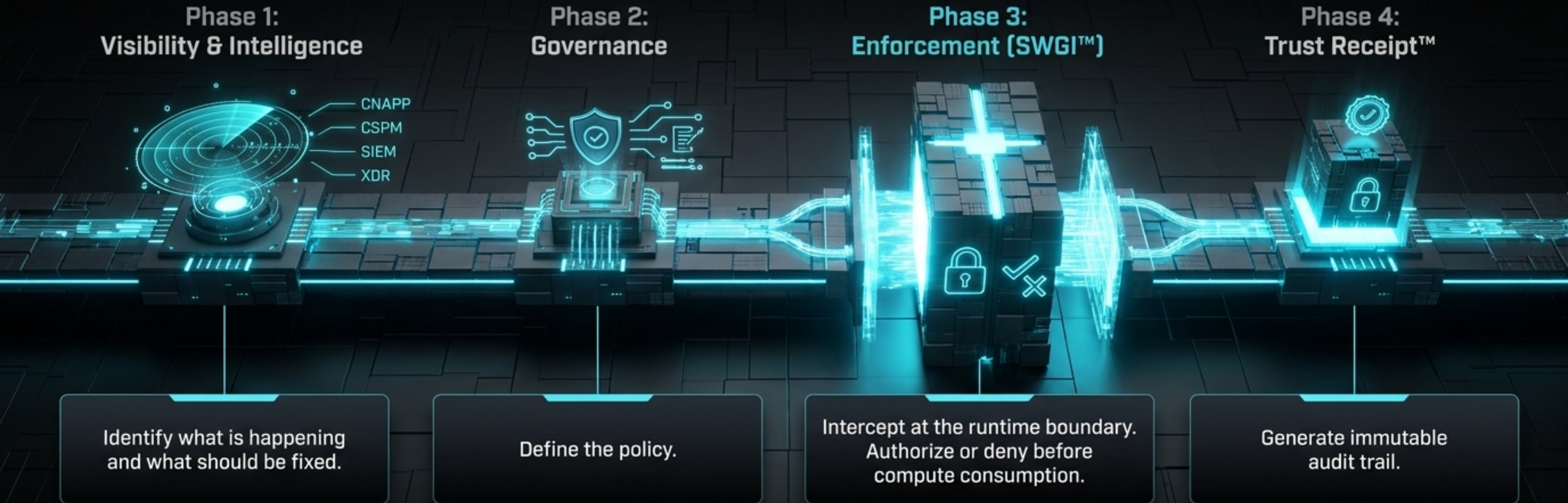


- Pre-execution gating
- Maximized work-per-watt
- Flattened unpredictable power spikes

Helps reduce erratic workload-driven power spikes and improve compute utilization, supporting data center efficiency, cooling capacity management, and alignment with high-density AI infrastructure goals.

Extending the Cloud Security Ecosystem

Traditional cloud-native security tools excel at telemetry and risk identification.
SWGITM acts as their deterministic enforcement arm.



While existing tools identify a **configuration drift**,
SWGITM prevents that risk from turning into runtime execution.

Built for High-Assurance Environments

Where deterministic execution is non-negotiable.



Sovereign AI & Agentic Governance

Enforces strict boundaries around sovereign data pools and multi-tenant agentic AI workflows. Prevents unauthorized API tool calls.



Critical Grid & Defense (DoD/DOE)

Secures grid controls and Industrial Control Systems (ICS) against unauthorized physical execution paths. Real-time safety cutoffs.



Tier-1 Financial Ledgers

Governs transaction processing and settlement infrastructure. Validates operational execution pathways before state changes trigger.

The Deployment Timeline

One-Click
Installation



Operator-Driven
Infrastructure Automation



Instant Fleet-Wide
Governance



Procurement & Deployment Readiness

Day 0 Ready. Fully automated operator architecture designed for rapid deployment without scaling complexity.

Approved Purchasing Vehicles

Google Cloud
Marketplace



Anthos Fleet
Management



Carahsoft (GSA MAS, NASA
SEWP, Army ITES-SW2,
NASPO ValuePoint)

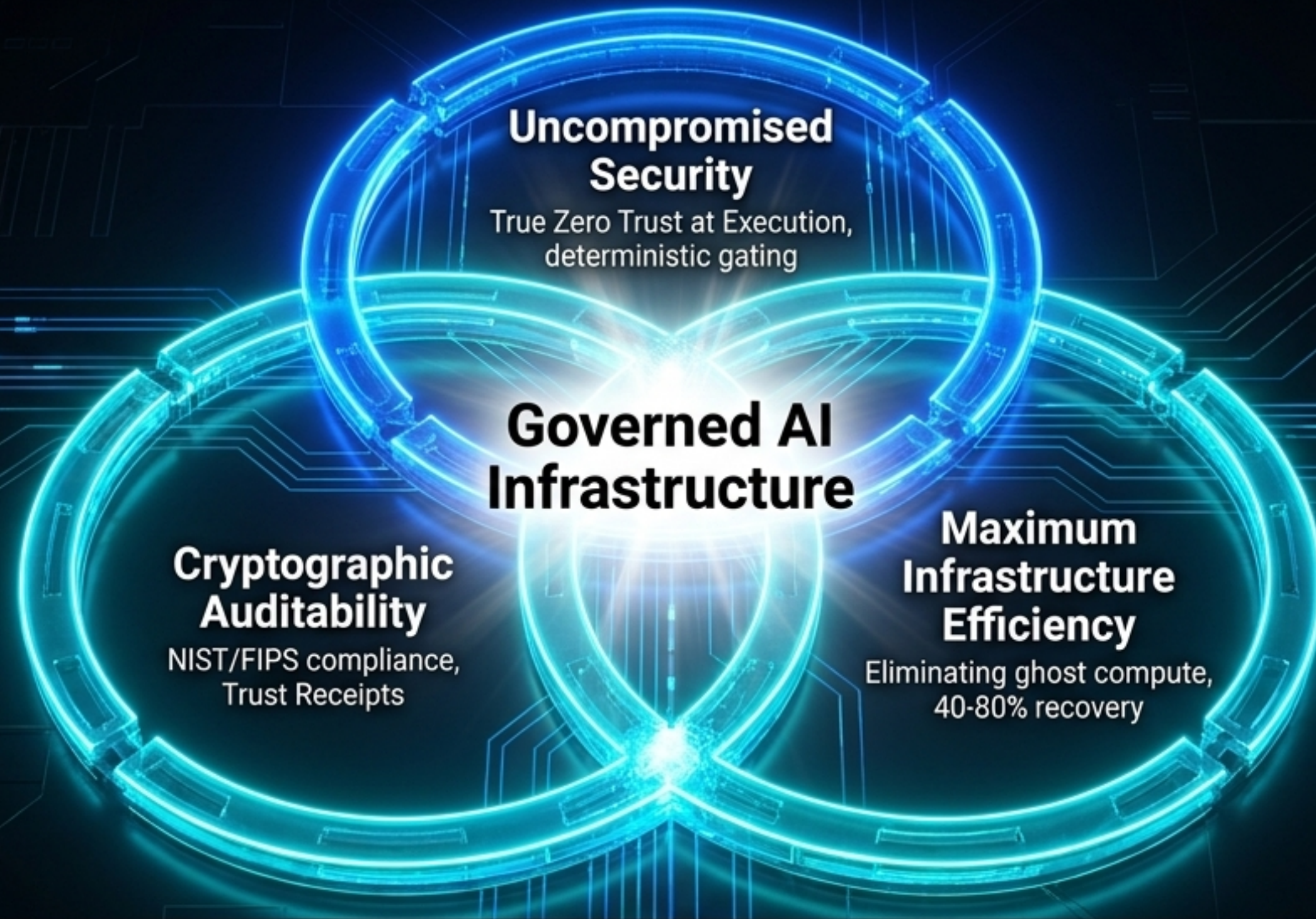


Intel Partner Alliance



Total Execution Accountability

Security, Compliance, and Sustainability are no longer separate tools; they are the exact same mechanism



“By integrating SWGI™ into the infrastructure fabric, organizations transform governance from a fragmented overhead task into a fundamental law of physics for the data center.”

The Future of AI Infrastructure is Governed Compute

As AI becomes more autonomous, the only safe infrastructure is governed infrastructure. The strategic objective is to make SWGI the default trust layer globally.

Vision:

Every substation, factory, and critical node operating AI workloads runs with AXIS-enabled hardware trust. Reduced risk, enforceable governance, and verifiable execution.



Govern Before Execution™

Google Cloud orchestrates infrastructure.
SWGI™ governs execution.
Trust Receipts™ prove authorization.

Execute = Instruction + Authority



Axis
Systems

Powered by
Intel Xeon 6

Google Cloud
Partner

Activate via Google Cloud Marketplace | Access the Interactive SWGI Sandbox