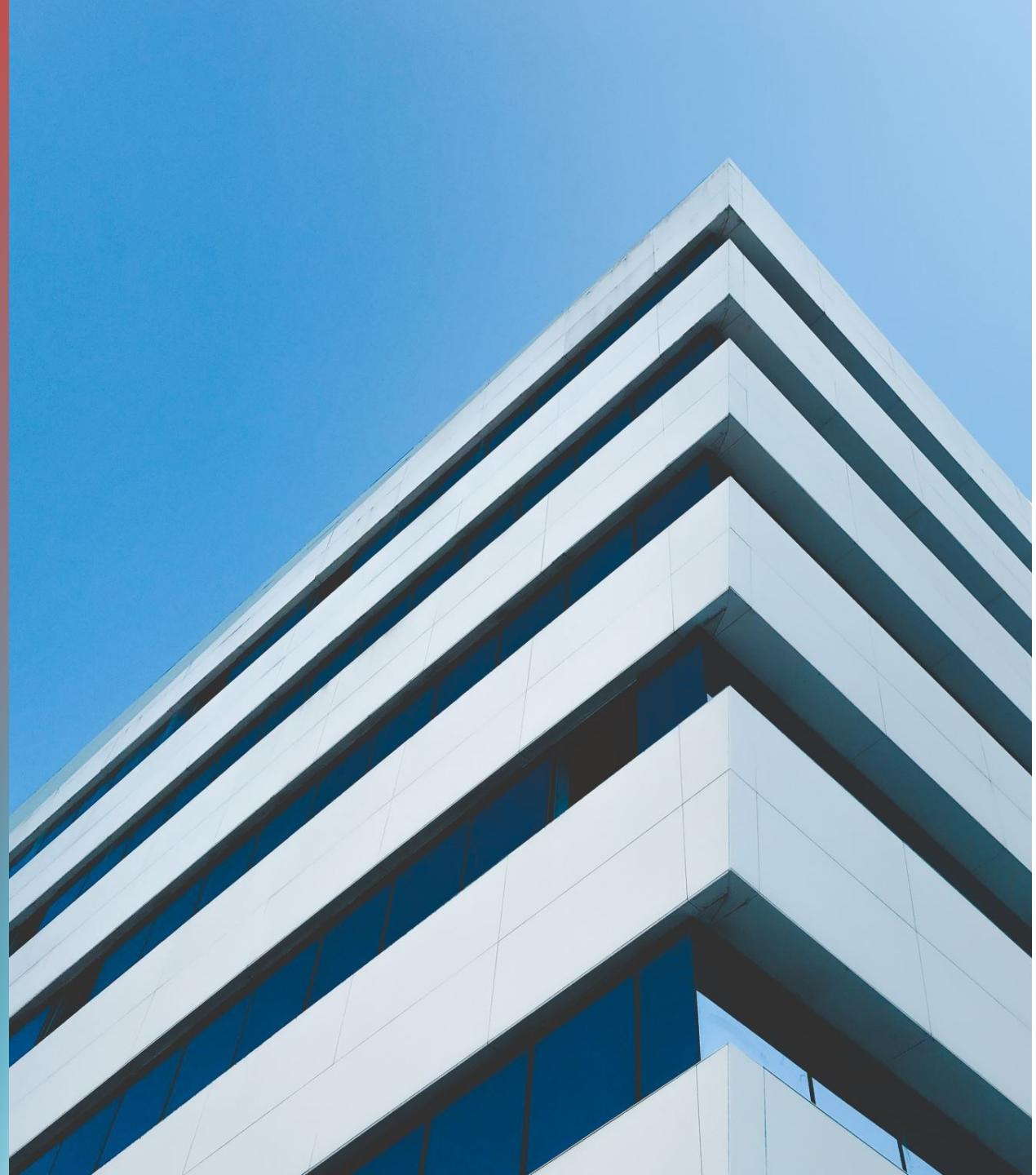
Douglas E. Farmer, Jr., CISSP

Architecting the future of identity-driven security

Principal Security Architect — Zero Trust • SSE/SASE • AI Governance

Patent: US-12432181-B2



Who I Am

I design and scale security architectures that become long-term operating models for regulated enterprises. My work centers on identity-centric enforcement, unified control planes, and architectural clarity that engineering teams can build on, and executives can trust.

What Most Enterprises Get Wrong About Security

Security complexity is not a tooling problem — it's an architectural one.

"The Mistakes"

- Security is still **network-centric**
- AI adoption is outpacing **governance models**
- Tool sprawl is replacing **architecture**
- Enforcement is fragmented across **platforms**
- Policies are static in a **dynamic world**

"The Reality"

- The Identity, not the network, must be the **control surface**
- AI requires **runtime governance**, not static controls
- Architecture must unify, not multiply tools
- Decisioning must be **centralized**, enforcement distributed
- Policy must be **adaptive, context-aware, and real-time**

"Most organizations are solving for coverage. I design for control."
This is what led me to design identity-centric control planes.

Architectural North Star

1. Identity is the control surface
2. Governance must be centralized; enforcement must be distributed
3. Architecture should reduce friction, not add it

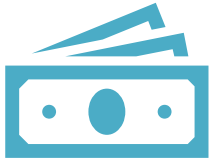
SASE Transformation

From Fragmentation to Unified Control Plane

- Unified SSE architecture across 80,000+ endpoints

- 75% reduction in incident escalations

- 50% improvement in application performance



- $1.8M annual operating expense reduction

Scope of Impact

Enterprise-scale architecture requires more than design — it requires alignment, influence, and execution.

1. Scale

- **80,000+** endpoints across enterprise environments
- Multi-line-of-business coverage
- **Global** user base and distributed workforce

2. Organizational Influence

- Aligned **Distinguished Engineers, Principal Architects, and platform owners**
- Led cross-organization architectural decision-making
- Resolved high-impact technical conflicts across teams

3. Strategic Ownership

- Defined long-term **SASE / SSE architectural direction**
- Influenced **multi-million dollar platform investments**
- Established enterprise-wide **security standards and patterns**

4. Business Impact

- $1.8M+ annual OpEx reduction
- 75% reduction in incident escalations
- 50% improvement in application performance
- Enabled scalable GenAI adoption across enterprise

Designed, led, and implemented division-level architecture

Identity-Centric Enforcement

Operationalizing identity as the enforcement layer

Defined division-wide identity enforcement patterns

Built rapid-response policy mechanisms enabling CSOC to deploy blocks in under 30 minutes

Influenced OS-level enforcement with Apple, Google, Broadcom

Aligned platform investments with long-term architectural direction

AI Governance & Agentic Control Planes

Extending the control plane to govern AI systems

EXTENDED SSE CONTROL PLANE TO GOVERN GENAI ADOPTION

BUILT DISTRIBUTED GUARDRAIL ARCHITECTURE

INTEGRATED CASB, DLP, PROXY TELEMETRY, SIEM PIPELINES

EMBEDDED LLM-ASSISTED WORKFLOWS INTO SECOPS

Case Study : SASE Modernization

Problem:
Fragmented proxy, CASB, and enforcement stack causing inconsistent governance, performance issues, and operational friction.

Approach:

- Defined long-term SASE strategy
- Unified eight security platforms into a single SSE control plane
- Aligned Distinguished Engineers and platform owners
- Consolidated regulatory + developer requirements into one scalable model

Outcome:

- 75% reduction in escalations
- 50% performance improvement
- $1.8M annual OpEx reduction
- SSE established as the division standard

Case Study: AI Control Plane

Problem:
Rapid GenAI adoption with no guardrails, no visibility, and high regulatory risk.

Approach:

- Extended SSE control plane to enforce identity-aware AI routing
- Built distributed guardrails to prevent data exfiltration + unauthorized agentic behavior
- Integrated CASB, DLP, proxy telemetry, and SIEM pipelines
- Created real-time AI usage visibility + risk scoring

Outcome:

- Safe, scalable GenAI adoption
- Shadow AI significantly reduced
- Real-time telemetry for AI usage patterns
- Architecture aligned with emerging regulatory expectations

How I Think About Security

- Security should enable, not restrict
- Risk must be understood in context
- Systems must align with real workflows
- Architecture should scale decision-making

Patent: Identity-Aware Proxy Enforcement

Problem

- Inconsistent enforcement across network environments
- Loss of identity context in hybrid architectures

Approach

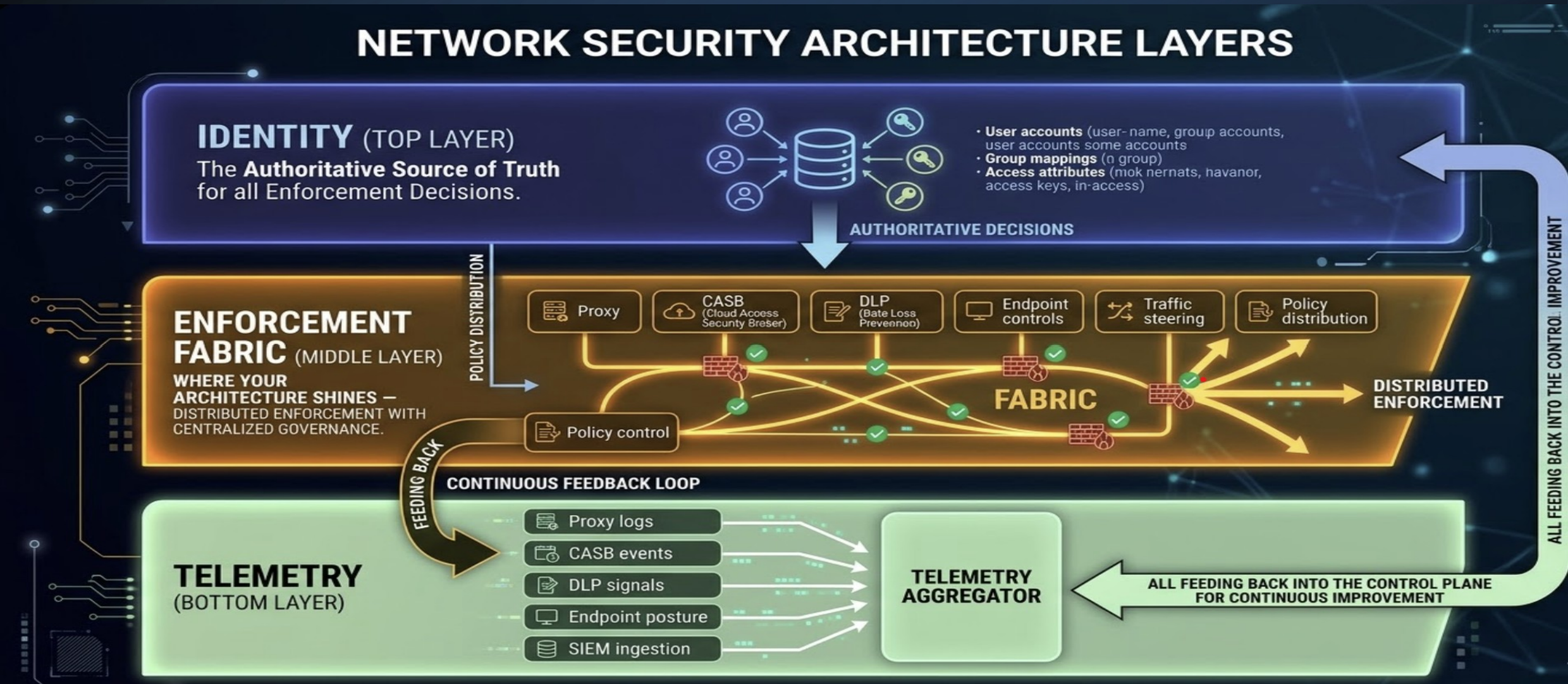
- Designed “always-on” identity-aware proxy model
- Removed reliance on network-based enforcement

Impact

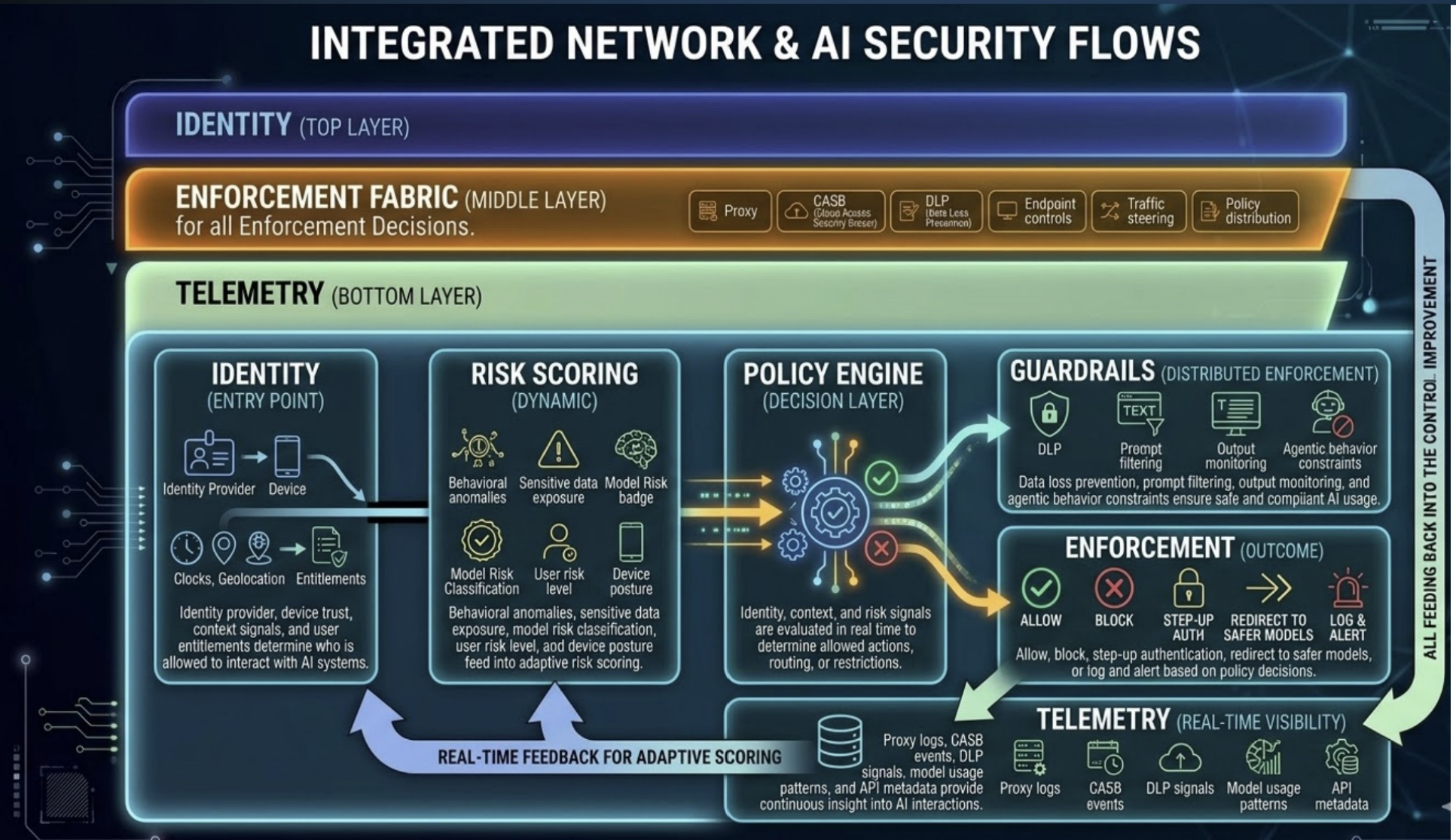
- Enabled consistent Zero Trust enforcement across environments
- Simplified enterprise security architecture
- Patent: US-12432181-B2

Identity-Centric Control Plane Model

"This is the model I use to scale security across enterprise environments."



Agentic AI Security Model



Identity (Entry Point)
Identity provider, device trust, context signals, and user entitlements determine who is allowed to interact with AI systems.

Guardrails (Distributed Enforcement)
Data loss prevention, prompt filtering, output monitoring, and agentic behavior constraints ensure safe and compliant AI usage.

Telemetry (Real-Time Visibility)
Proxy logs, CASB events, DLP signals, model usage patterns, and API metadata provide continuous insight into AI interactions.

Risk Scoring (Dynamic)
Behavioral anomalies, sensitive data exposure, model risk classification, user risk level, and device posture feed into adaptive risk scoring.

Policy Engine (Decision Layer)
Identity, context, and risk signals are evaluated in real time to determine allowed actions, routing, or restrictions.

Enforcement (Outcome)
Allow, block, step-up authentication, redirect to safer models, or log and alert based on policy decisions.

"This is the model I use to scale security across enterprise environments."

How I Lead

- I align senior engineers and executives around shared direction
- I resolve high-stakes architectural disagreements
- I create clarity across fragmented systems
- I mentor and elevate senior engineers and architects
- I drive decisions that balance risk, speed, and scale

I value clarity, consistency, and showing up for the people I work with

“What I Bring”

At my core, I bring:

- Define enterprise-scale security architecture
- Align engineering execution with executive strategy
- Deliver measurable business impact
- Lead forward-looking AI + identity security models