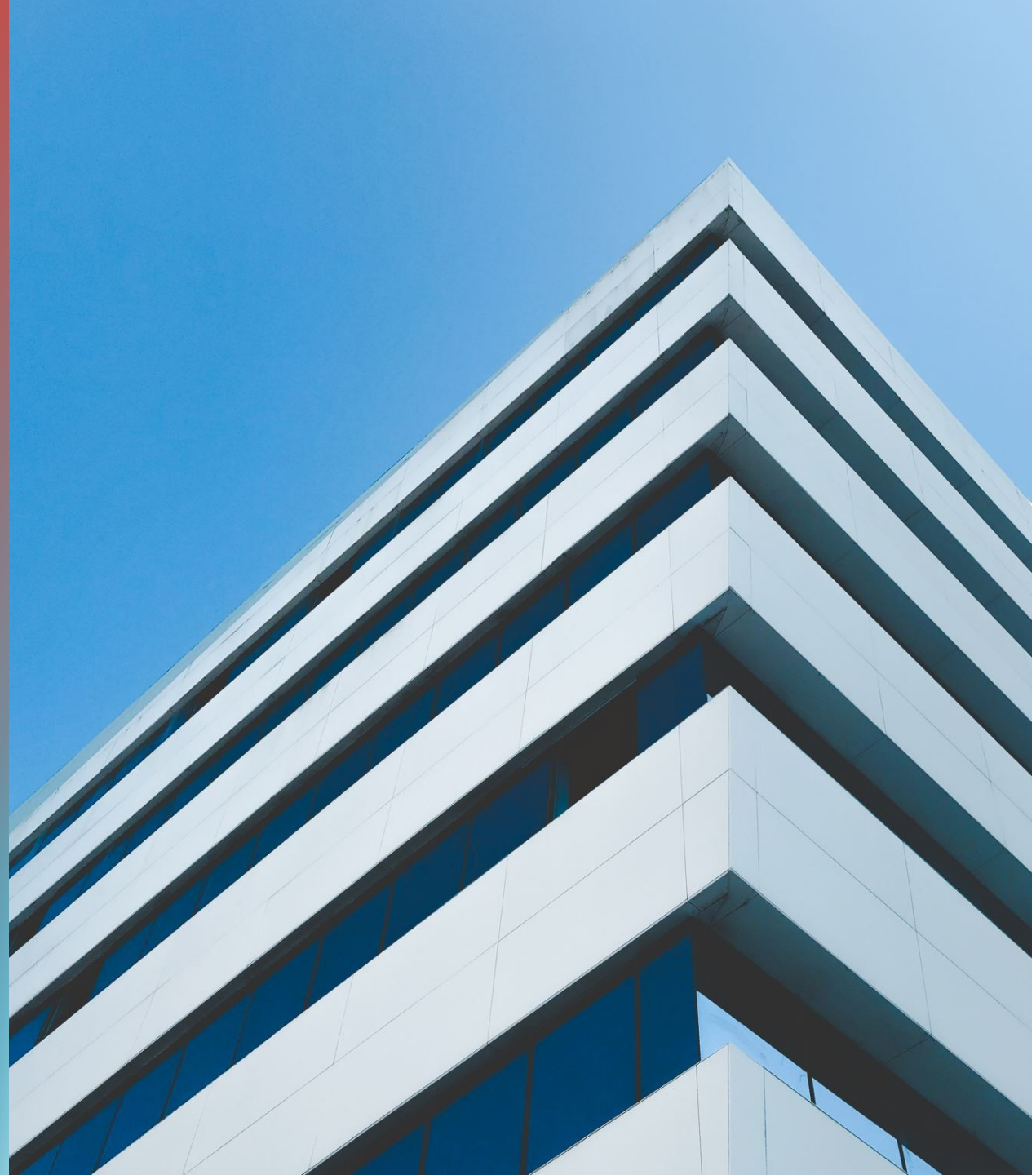
Douglas E. Farmer, Jr., CISSP

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

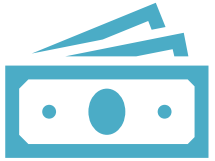
SASE Transformation

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

These ideas directly inform the architecture models I use to scale security.

Solving the Split-Brain Proxy Problem
(Patent US-12,432,181-B2)

THE CHALLENGE

- SaaS proxy agents disable themselves on corporate networks
- Creates two enforcement domains and inconsistent policy
- Identity context is lost when agents enter “passive mode”

  “This ‘passive mode’ behavior results in inconsistent policy enforcement, lost user identity context…”

THE INNOVATION

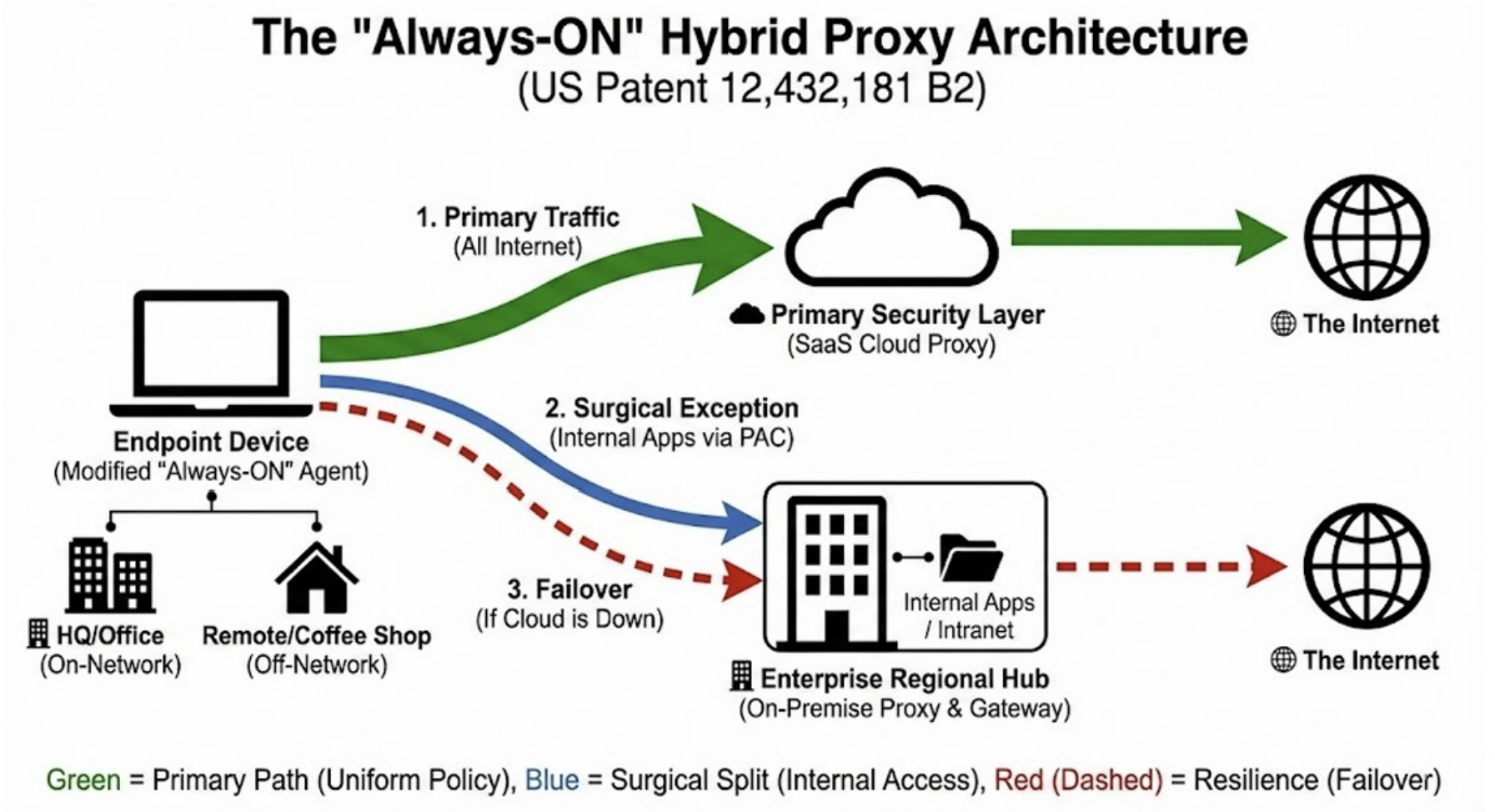
- Patented “Always-ON” architecture forces a uniform cloud path
- Modified agent removes all network-location awareness
- Cloud proxy becomes the primary enforcement layer everywhere

HOW IT WORKS

- All traffic → SaaS proxy (on-network + off network)
- PAC file provides surgical internal routing
- On-prem hardware becomes failover, not primary

WHY IT MATTERS

- Universal Policy Enforcement (UPE)
- Location-agnostic Zero Trust
- Simplifies hybrid security at enterprise scale



(Caption: The "Always-ON" architecture forces a primary cloud path while preserving surgical access to internal apps.)

Modernizing Proxy Logic for SPAs & Dynamic Apps

(Header-Aware, Intent-Based Inspection)

THE CHALLENGE

- Legacy 302 redirects break modern SPAs
- Background fetch requests receive HTML login pages

THE SOLUTION

- Header-aware inspection using
- Distinguish human navigation vs. background API calls
- Validate session cookies before triggering authentication

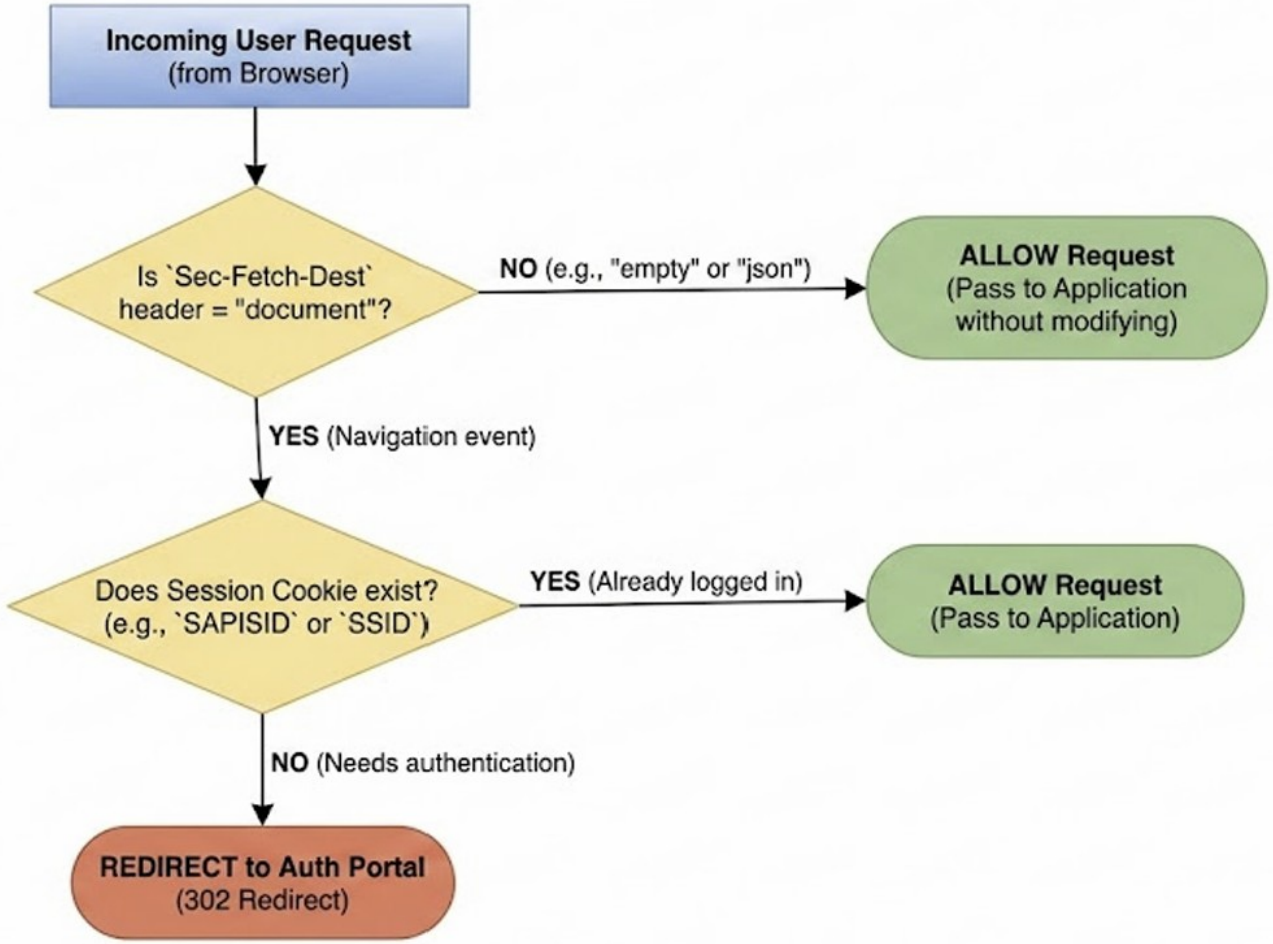
SMART LOGIC

- **DOCUMENT** → Human navigation → Redirect allowed
- **Empty/json**→ Background call → Never redirect
- Session cookie present → Allow
- Cookie missing → Trigger auth (only for humans)

OUTCOME

- No infinite loops
- No broken SPAs
- Strong authentication preserved
- Better UX, better stability

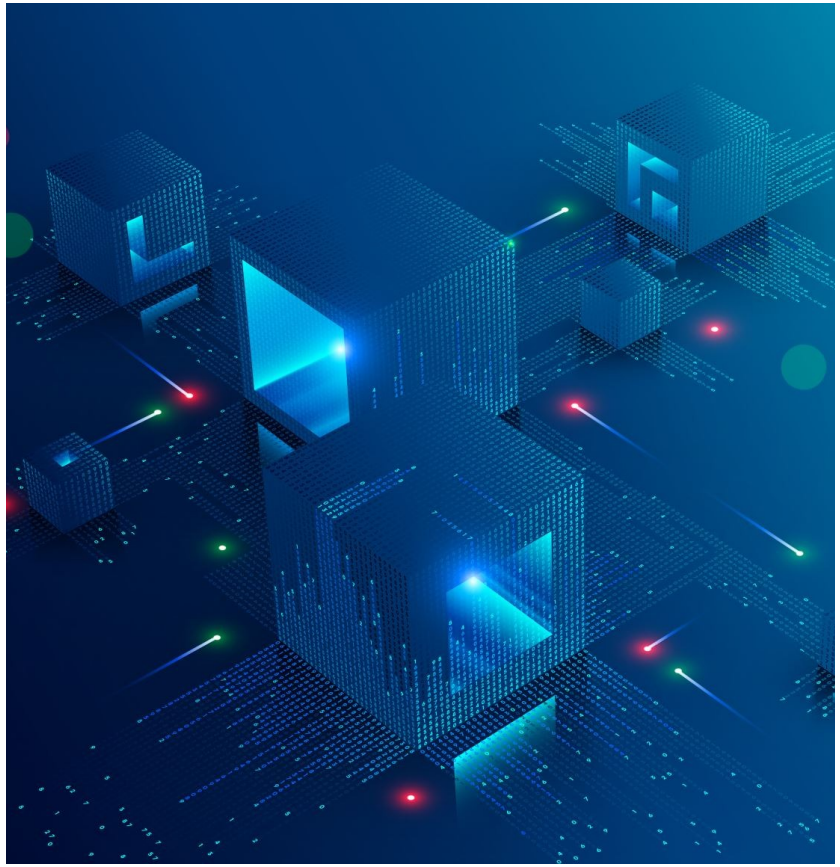
Smart Proxy Logic Flowchart (Header-Aware)



Zero Trust Architecture

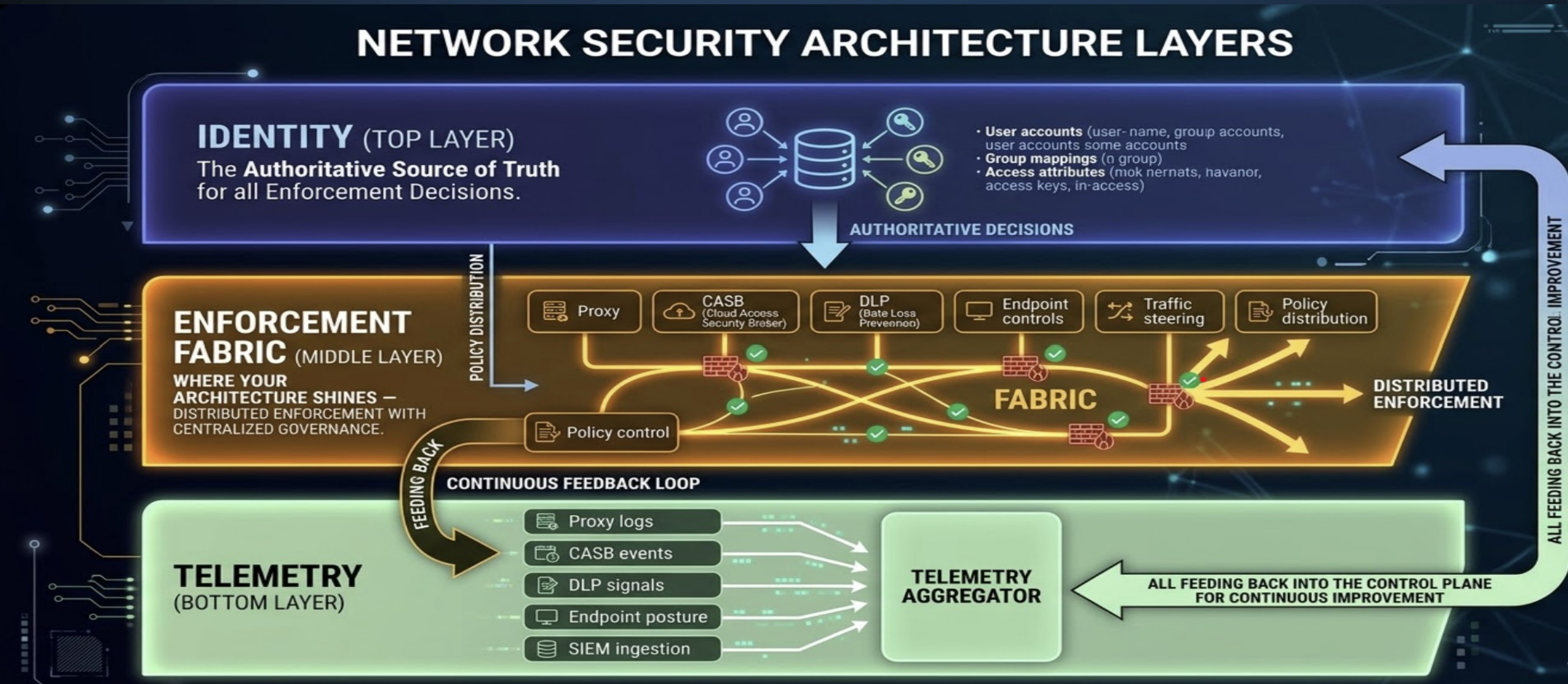
Principles:

- Identity-first enforcement
  Identity is the primary decision surface across network, SaaS, and AI interactions.
- Continuous verification
  Every request is validated based on identity, device posture, context, and risk.
- Context-aware access
  Policies adapt dynamically to user behavior, device state, and environmental signals.
- Policy-driven segmentation
  Access is granted based on least privilege and enforced through centralized governance.
- Unified telemetry and decisioning
  Signals from proxy, CASB, DLP, endpoint, and identity feed a single control plane.

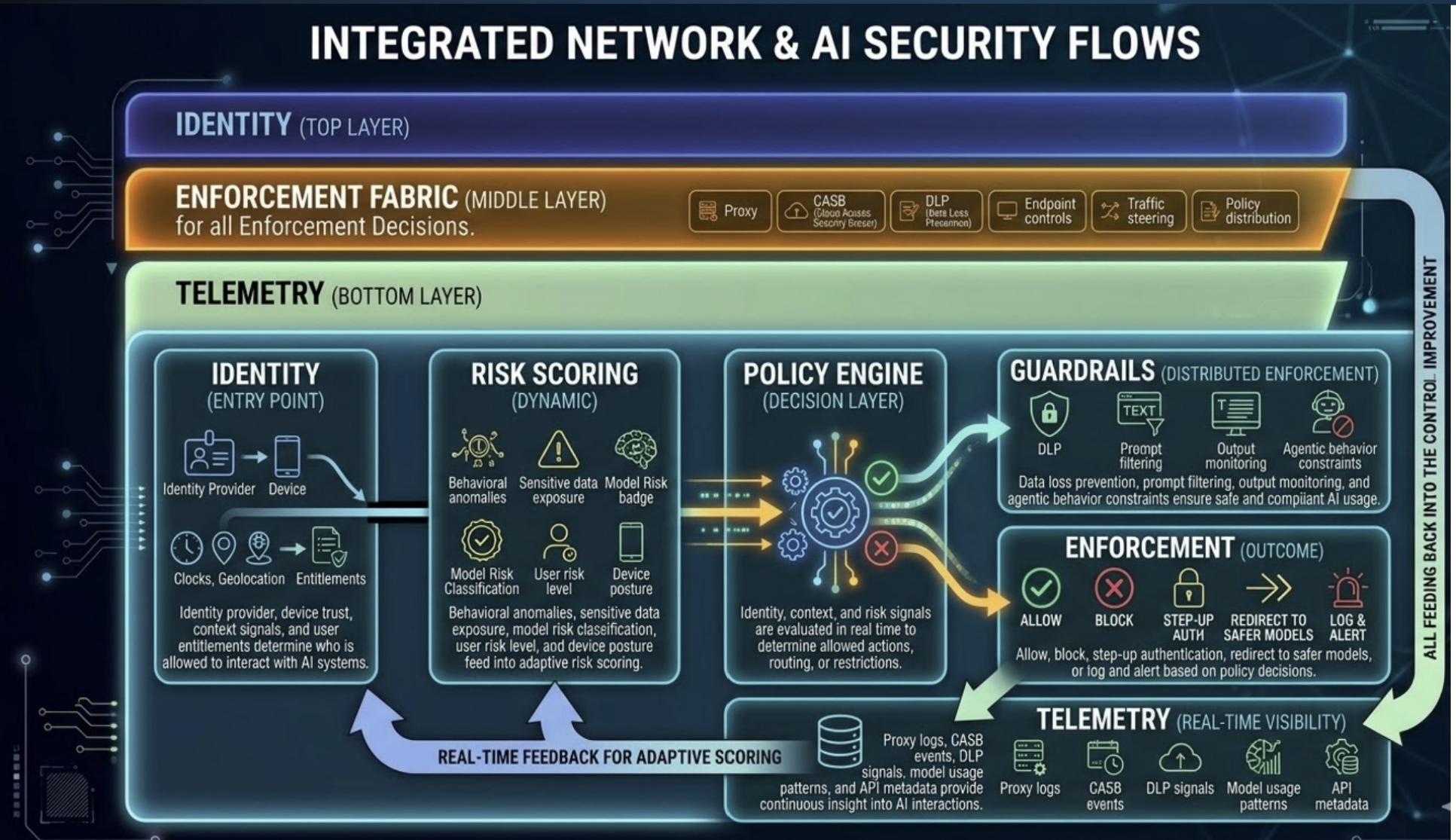


Identity-Centric Control Plane Model

"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

How I Work Under Pressure

- I’m the calm one in the room when chaos hits
- I prefer strategy over noise — root cause over symptoms
- I hyper-focus on complex or “unsolvable” problems
- I pull in colleagues to sharpen thinking
- I stay steady, thoughtful, and solutions-oriented

My Why

Everything I do — professionally and personally — is rooted in presence, honesty, and care. I show up for my family the same way I show up for my teams: steady, thoughtful, and committed to doing what’s right.

Family is the center of my world. My purpose is to ensure the people I love feel safe, supported, and valued. Integrity isn’t a value — it’s a way of life. You’re only as good as your word.

What Brings Me Joy

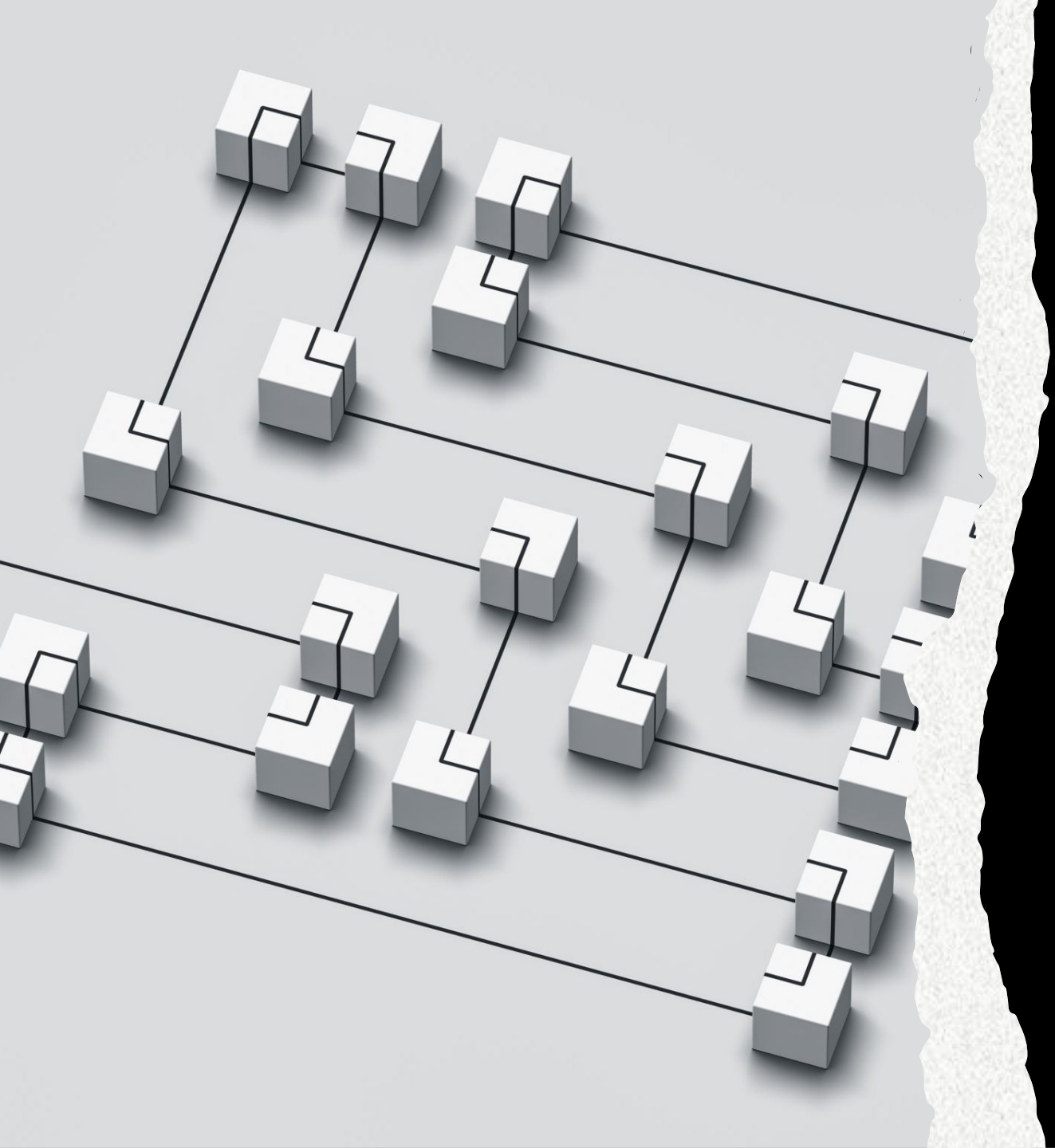
- Avid console gamer
- Lover of books
- Eclectic music taste (80s, 90s, early 2000s are the golden eras)
- Late-bloomer traveler who loves exploring with my kids
- Dog person — Bo is my shadow

I'm happiest when I'm exploring new places with my family, finding quiet moments, and appreciating the world beyond the screen.

“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



What I’m Looking For

- Shape long-term architectural direction
- Influence platform strategy
- Build scalable, identity-driven security systems
- Partner with leaders to drive transformation
- Help teams grow, align, and succeed

Thank you for taking the time to get to know me — both the architect and the human.