Douglas E. Farmer, Jr.

Upper Marlboro, MD | (202) 207-4641
douglas.farmer@gmail.com | linkedin.com/in/douglasfarmerjr | **Patent ID: US-12432181-B2**

PRINCIPAL SECURITY ARCHITECT - STRATEGY, INFRASTRUCTURE & AI GOVERNANCE

Zero Trust & SSE Architecture | Agentic AI Control Planes | Enterprise Scale (80k+ Endpoints) | U.S. Patent Holder

PROFESSIONAL SUMMARY

I design and scale security architectures that enable organizations to understand, manage, and reduce risk at enterprise scale. Over the past decade, I have led division-level Zero Trust and SASE transformations, translating complex regulatory and technical challenges into scalable systems that balance security, business velocity, and user experience.

My work centers on identity-centric enforcement and unified control planes that align engineering execution with strategic risk management. I define long-term architectural direction, align senior engineering leaders, and guide security and risk decisions that executives can confidently support.

CORE EXPERTISE

- Zero Trust Architecture and Identity-Centric Enforcement
- SASE and SSE Strategy and Multi-Platform Integration
- Division-Level Security Modernization Programs
- AI Governance and Generative AI Guardrails
- CASB, SaaS Risk Governance, and Shadow IT Discovery
- Multi-Tenant Security Architecture
- M&A Integration, Vendor Platform Strategy, and Technical Due Diligence
- FedRAMP, STIG, and RMF-Aligned Design

STRATEGIC RISK & BUSINESS ALIGNMENT

- Serve as a strategic advisor to engineering and business leadership on security risk, architectural tradeoffs, and long-term platform direction
- Translate regulatory and compliance requirements into scalable technical controls aligned with business velocity
- Define and evolve enterprise risk posture across network, SaaS, and AI environments
- Align security architecture with developer workflows and operational priorities to reduce friction while maintaining strong control

PATENTS & CERTIFICATIONS

- **U.S. Patent [US-12432181-B2]:** SASE Control Scheme & Traffic Steering – Foundational mechanism for Zero Trust/SASE and IDE Routing.
- Symantec SASE & Proxy Ecosystem Industry Expert (formerly Blue Coat Certified Trainer)
- **Certifications:** CISSP, AWS CCP, Security+, ITIL v3

PROFESSIONAL EXPERIENCE

CAPITAL ONE | McLean, VA **Senior Lead Platform Engineer (*Division-Level Security Architecture & Risk Strategy*)** | May 2018 – Present

Serve as architectural lead for a division-level SASE and Zero Trust modernization initiative spanning approximately 80,000 Windows and macOS endpoints across multiple Lines of Business. The program replaced fragmented proxy and CASB infrastructure with a unified identity-driven control plane and established SSE as the division standard for network and SaaS enforcement.

Division-Level SASE Transformation (Multi-Year)

- Partnered with engineering and business stakeholders to align security architecture with operational workflows, enabling secure delivery without impacting velocity.
- Defined the long-term SASE architectural strategy and target state operating model for the division.
- Drove executive-aligned architecture strategy that secured division funding for long-term SASE modernization.
- Defined the enterprise SSE reference architecture integrating proxy, CASB, DLP, endpoint, identity, and telemetry systems across eight security platforms.
- Led proof-of-concept evaluations, vendor selection, and technical due diligence for enterprise-wide SSE adoption.
- Consolidated regulatory, operational, and developer requirements across multiple Lines of Business into a unified scalable architecture.
- Directed division-level architectural delivery alongside four Distinguished Engineers, aligning cross-platform decisions and resolving high-impact technical disputes.
- Migrated legacy CASB infrastructure into the unified SSE stack, eliminating redundant controls and simplifying governance across more than 80,000 endpoints.
- Reduced operational risk exposure by 75% following SSE standardization.
- Improved application performance by ~50% through traffic steering optimization, while reducing user friction and enabling secure developer workflows.
- Delivered $1.8M+ in sustained annual operating expense reduction through architectural simplification and vendor rationalization aligned with long-term strategy.
- Established the SSE control plane as the **long-term architectural standard** for division-wide network, SaaS, and identity-aware enforcement, forming the foundation for future AI governance patterns.
- Defined architectural principles now used as the baseline for new security platform integrations.

Architectural Governance and Technical Direction

- Served as senior escalation authority for high-risk architectural decisions affecting multiple engineering organizations.
- Communicated architectural strategy and risk tradeoffs to senior leadership, enabling informed decision-making across complex environments.
- Led a cross-organization steering committee composed of Distinguished Engineers, Principal Architects, and platform owners, **driving architectural alignment across independent engineering organizations and resolving competing technical approaches.**
- Defined identity-centric enforcement patterns that reduced policy fragmentation and enabled consistent risk management across network and SaaS environments.
- Instituted rapid-response policy mechanisms enabling CSOC teams to deploy high-priority threat blocks in under 30 minutes without destabilizing broader architecture.
- Influenced OS-level network enforcement capabilities through direct collaboration with engineering teams at Apple, Google, and Broadcom, shaping platform behaviors that enabled enterprise-scale identity-aware traffic control patterns.
- Owned vendor strategy and multi-million-dollar platform investments, aligning commercial decisions with long-term architectural direction.

AI Control Plane Architecture and Governance

- Advised on GenAI risk exposure and implemented guardrail architecture enabling safe adoption across engineering and business environments
- **Extended the enterprise SSE control plane** to govern generative AI adoption across developer and business environments, integrating identity, proxy enforcement, and telemetry pipelines into a unified policy model.
- Established distributed guardrail architecture preventing data exfiltration, unauthorized agentic behavior, and shadow AI adoption while preserving developer velocity.
- Extended the existing SSE control plane to support AI-aware routing, SaaS discovery, and risk scoring across more than 80,000 endpoints.
- Integrated CASB, DLP, proxy telemetry, and SIEM pipelines into a centralized enforcement framework enabling real-time visibility into GenAI usage patterns.
- Established scalable architectural patterns for safe GenAI adoption by translating emerging regulatory expectations into reusable engineering controls.
- Embedded LLM-assisted workflows into security operations pipelines to accelerate investigation, threat modeling, and incident response decision cycles.

CAPITAL ONE | McLean, VA **Lead Platform Engineer** | May 2014 – May 2018

- Architected zero-downtime migration of enterprise proxy traffic from physical data centers to virtual private cloud, achieving 99.999 percent uptime.
- Designed authentication mechanisms that improved developer workflow efficiency and reduced friction.
- Recognized with multiple TechX awards for enterprise innovation and modernization impact.
- Established internal architectural documentation standards that simplified proxy and security platform adoption across engineering teams.

GENERAL DYNAMICS IT (GDIT) | Fort Meade, MD **Senior Security Engineer (Federal/DoD)** | 2013 – 2014

- Led security architecture for Secret-level coalition networks supporting multinational defense operations.
- Designed DISA-compliant architectures aligned with STIG and RMF requirements.
- Reduced infrastructure provisioning timelines by 25 percent through deployment modernization.
- Served as global technical lead for enterprise security ecosystems including Blue Coat and Palo Alto platforms.

PUBLIC DEFENDER SERVICE FOR DC | Washington, D.C. **Lead IT Specialist** | 2012 – 2013

- Acted as technical advisor to senior leadership on modernization strategy and security posture improvement.
- Designed a roadmap for transition to cloud-based messaging infrastructure.
- Reengineered IT service processes resulting in measurable reduction in mean time to resolution.

EARLY CAREER & PRIOR EXPERIENCE

- **IT Security Engineer & Certified Trainer**, Braxton Grant Technologies (2011–2012) – Principal Blue Coat Authority
- **IT Specialist**, Public Defender Service for DC (2008–2011)
- **Additional Technical Roles** (2004–2008): Includes positions at US Dept of Justice, US Census Bureau & Pension Benefit Guaranty Corp.

ARCHITECTURE & TECHNICAL DOMAINS

- **Security Architecture:** Zero Trust Architecture, AI-Augmented DevSecOps, Agentic Control Planes, SSE/SASE Design, Custom Policy Architecture (CPL/XML/JSON), GenAI Security Governance, LLM Risk Mitigation, Identity & Access Management (IAM), Mobile Device Management (MDM).
- **Cloud & Infrastructure:** AWS, GCP, Azure, Advanced Proxy Logic & Traffic Forensics, Developer Experience (DX) Optimization.
- **Platforms:** Zscaler, Netskope, Palo Alto Networks, Broadcom/Symantec (Blue Coat), Microsoft Entra ID (Azure AD).
- **OS & Protocols:** macOS Network Extensions, Windows Filtering Platform (WFP), OIDC, OAuth2, SAML, FIDO2/WebAuthn (Passwordless).