

RONNIE BAILEY

Richmond, VA | (804) 803-1311

opportunities@ronniebailey.cloud | linkedin.com/in/ronniebailey

Principal Cybersecurity & IAM Architect with 13+ years securing hybrid cloud environments for Fortune 500 and federal clients. Expert in Zero Trust, PAM, identity Governance, and secure cloud transformations that reduce risk and enhance compliance. Proven track record delivering enterprise IAM solutions that enable business goals.

PROFESSIONAL EXPERIENCE

THREAT DETECTION/IAM AUTOMATION ARCHITECT

LexisNexis & United States Patent and Trademark Office (Contract) | 2024–Present

**Public Trust Clearance*

- Threat Detection Integration: Engineered solutions using CrowdStrike Falcon, Microsoft Defender, Palo Alto, and Checkpoint Identity Security, correlating telemetry across platforms to reduce incident response time by 90%.
- Zero Trust Implementation: Constructed framework with Just-In-Time provisioning and risk-based authentication, reducing standing privileges by 60% while implementing continuous authentication monitoring aligned with NIST 800-207.
- Privileged Access Management: Utilized One Identity Safeguard, Secureworks Taegis, and Sophos MDR in tandem to monitor privileged sessions, detect anomalous behavior, and respond to threats across 500+ hybrid systems.
- IAM Modernization: Migrated legacy platforms to Microsoft Identity Platform and Okta, enabling FIDO2/WebAuthn passwordless authentication, adaptive MFA, and lifecycle automation using PowerShell and Python for 15,000+ users.
- Federated Authentication Integration: Integrated Auth0 into enterprise IAM stack to enable OAuth2/OpenID Connect-based SSO across internal apps, supporting FedRAMP and NIST 800-53-compliant authentication workflows.
- Digital Forensics: Designed and executed forensic response plans using Secureworks Taegis and The Sleuth Kit, implementing NIST 800-86-aligned chain-of-custody workflows to preserve evidence integrity.
- Cloud Security: Led Azure security blueprint development, integrating NIST 800-53, CIS, and HIPAA frameworks, while automating compliance validation and reporting workflows across Microsoft 365.

- Multi-Cloud Security: Implemented consistent security controls and policy enforcement across AWS, Azure, and GCP environments with centralized CSPM integration and automated misconfiguration detection.
- Identity Governance: Unified fragmented IAM tools into enterprise-wide architecture using One Identity, ADManager Plus, and Microsoft Entra ID with AI-driven identity analytics and policy-based provisioning.
- Microsoft 365 Security: Overhauled Exchange Online with DLP, data classification, and conditional access policies to mitigate insider threats and enforce Zero Trust access principles.

IAM SECURITY ARCHITECT, CYBERSECURITY

Kroger, Technology & Digital Department | 2022–2024

- Privileged Access Security: Implemented Onedidentity Safeguard/TPAM, aligning workflows with NIST 800-53 within 6 months and incorporating just-in-time privilege elevation.
- Endpoint Protection: Deployed CrowdStrike Falcon, reducing malware incidents by 45% across 2,000+ endpoints.
- Cloud Identity Management: Engineered security modernization using Entra ID/Azure AD for 12,000+ hybrid users with Kubernetes service identity integration.
- Virtualization Strategy: Standardized infrastructure using VMware vSphere across production and test environments, improving system uptime and reducing operational costs through centralized VM lifecycle management.
- Container Security: Designed pod identity solution for Azure Kubernetes Service (AKS), eliminating the need for static credentials in containerized applications.
- Authentication Modernization: Integrated Okta SSO/MFA across 40+ apps, implementing risk-based authentication, and reducing password-reset tickets.
- Access Control: Streamlined Active Directory with RBAC/conditional access, cutting unauthorized access by 30%.
- Account Lifecycle Management: Automated processes ensuring HIPAA compliance for 20,000+ accounts.
- Global Identity Provisioning: Led implementation for 32,000+ users across US/UK teams, cutting onboarding time by 55%.
- Data Governance: Enhanced security with Varonis, improving audit readiness for SOX/GDPR compliance.

CUSTOMER IDENTITY & ACCESS MANAGEMENT ARCHITECT

Department of Homeland Security (DHS), OCIO – US Secret Service | Contract | 2022

**Public Trust Clearance*

- Privileged Access Management: Streamlined CyberArk's PAM workflows, achieving 100% compliance with NIST 800-53.
- Network Security: Deployed Fortinet FortiGate firewalls and micro-segmentation, achieving full CISA Zero Trust compliance.
- Enterprise IAM Strategy: Positioned IAM as the cornerstone of DHS security, integrating Active Directory, OAuth 2.0, and SAML 2.0 for 100+ legacy systems.
- Serverless Security: Implemented secure identity practices for serverless functions in GCP, enabling principle of least privilege with function-level permissions.
- Risk-Based Access Control: Mapped 75+ systems to business-criticality tiers, reducing high-risk privileged accounts by 35%.
- Cloud Migration Security: Orchestrated GCP migration for 50+ on-premises systems, enabling FedRAMP Moderate authorization with comprehensive SIEM integration.
- Identity Governance: Enforced granular access policies via Saviynt across 15,000+ user accounts.
- Security Certification: Spearheaded ISO 27001 certification for DHS's Information Security Management System.
- Agile Development: Utilized Agile, SCRUM, and scripting languages (PowerShell, Python, Java) to enhance system resilience and efficiency in alignment with FISMA compliance and security standards.

CLOUD VULNERABILITY ANALYST

Accessia Health | Contract | 2021

- Single Sign-On Implementation: Deployed PingFederate and Citrix NetScaler with 99.9% uptime for healthcare applications.
- Privileged Access Security: Spearheaded CyberArk implementation with NIST 800-53-aligned credential vaulting.
- Threat Detection: Engineered Microsoft Defender for Identity integration, reducing unauthorized access incidents by 75%.
- Cloud-Native Security: Implemented identity-aware proxies and service meshes for securing microservices architecture in AWS.
- Identity Architecture: Designed framework integrating Azure AD and PingFederate for 5,000+ hybrid identities.

- Behavioral Authentication: Implemented user and entity behavior analytics (UEBA) to detect compromised credentials and insider threats.
- Secure Communications: Modernized SSL/TLS protocols for 150+ domains, maintaining 100% compliance.
- Risk Management: Led vulnerability assessments aligned with NIST 800-53 and HIPAA standards.
- Compliance Automation: Implemented reporting via PingFederate logs for SOX, GDPR, and HIPAA audits.

PRIVILEGED ACCESS MANAGEMENT ARCHITECT

Indivior Pharmaceuticals | Contract | 2019–2021

- Privileged Account Security: Deployed BeyondTrust PAM, securing 1,200+ privileged accounts with SOX-compliant audit controls.
- Conditional Access: Architected role-based, location-based, and device-compliance policies in Microsoft Entra ID.
- Cloud Security: Designed GCP security framework using Google IAM and Security Command Center for real-time threat detection.
- SSO & MFA Integration: Integrated Azure AD/Entra ID to enhance user verification and streamline access management.
- Data Protection: Implemented BitLocker encryption and backup policies to safeguard ePHI across all endpoints.
- Continuous Authentication: Implemented risk-based authentication with context-aware access policies to dynamically adjust security requirements.
- Infrastructure-as-Code Security: Integrated security guardrails into Terraform deployments, ensuring compliance from deployment to runtime.
- Identity Lifecycle Management: Engineered SailPoint provisioning/deprovisioning workflows for 500+ employees.
- Identity Governance: Led SailPoint IdentityNow implementation, enabling centralized governance for distributed workforce.
- Least Privilege Implementation: Mapped 200+ job functions to least-privilege roles, eliminating segregation-of-duties conflicts.
- Mobile Device Security: Designed IAM solutions using Microsoft Intune for secure mobile device management and remote access enforcement.
- Endpoint Protection: Maintained Carbon Black for threat hunting, policy enforcement, and incident response.

IDENTITY AND ACCESS MANAGEMENT ANALYST

Wells Fargo | Contract | 2019

- Zero Trust Architecture: Designed the bank's first Zero Trust-aligned IAM framework, reducing policy exceptions by 35%.
- Security Automation: Leveraged Microsoft Defender's auto-remediation capabilities, cutting manual SOC tasks by 30%.
- Customer Authentication: Engineered progressive profiling workflows using ADFS with 99.9% portal uptime.
- Multi-Cloud Security Governance: Implemented consistent identity controls across AWS and Azure environments.
- Regulatory Compliance: Enforced FFIEC and GLBA requirements via SCCM and Office 365 access controls.
- Identity Management: Maintained 12,000+ user accounts across hybrid environments through automated lifecycle workflows.
- Security Training: Conducted staff education on best practices, reducing phishing incident response time.

CUSTOMER IDENTITY & ACCESS MANAGEMENT ENGINEER

Wellsecured IT | Contract | 2015–2019

- IAM Transformation: Led migration to ForgeRock Identity Management, standardizing identity lifecycle workflows for hybrid environments.
- Access Control: Architected conditional access policies using Microsoft Defender for privileged account management.
- Security Monitoring: Integrated Splunk with IAM tools, achieving ISO/IEC 27001 and NIST 800-53 compliance.
- API Security: Implemented OAuth 2.0 and OpenID Connect protocols for securing cloud-native application APIs.
- Cloud Identity Security: Built AWS IAM roles and encryption protocols across multi-cloud environments.
- Secure Access Solutions: Designed Citrix-based security for financial services clients' mission-critical applications.
- Customer Authentication: Spearheaded Auth0 integration for client-facing portals, balancing security with user experience.
- Security Automation: Partnered with DevOps teams to streamline log analysis and incident response.

CLOUD SECURITY OPERATIONS LEAD

Cloudcentria Security | Contract | 2011–2015

- Threat Response: Neutralized multi-vector DDoS attacks targeting financial sector clients with 99.99% uptime.
- Identity Integration: Pioneered Azure AD patterns for hybrid environments, adopted by Microsoft partner network.
- Digital Forensics: Led investigation recovering stolen intellectual property, establishing cloud evidence handling protocols.
- Cloud Workload Protection: Implemented comprehensive security for IaaS, PaaS, and serverless deployments across AWS environments.
- Compliance Management: Developed NIST 800-53 and ISO 27001-aligned policies with 100% audit success.
- Vulnerability Management: Scaled Nessus-based assessments to 15,000+ assets in AWS/Azure infrastructure.
- Authentication Unification: Integrated Ping Identity with Okta across SaaS platforms, reducing helpdesk requests.
- Security Training: Educated analysts in Kali Linux penetration testing methodologies for cloud environments.

KEY PROJECTS

ENTERPRISE-WIDE ZERO TRUST TRANSFORMATION

Department of Homeland Security | 2022

- Led cross-functional team implementing Zero Trust Architecture across 200+ mission-critical applications. Developed comprehensive security architecture incorporating micro-segmentation, just-in-time access, continuous verification, and least privilege enforcement. Reduced lateral movement risk by 80% while cutting incident response time by 60%. Project completed 3 months ahead of schedule, establishing new security baseline for federal systems.

MULTI-CLOUD IAM CONSOLIDATION

Kroger, Technology & Digital | 2023

- Unified disparate identity systems during migration to hybrid cloud environment spanning AWS and Azure. Designed cloud-native IAM solution with centralized governance, automated workflows, and identity analytics. Reduced operational costs by \$1.2M annually while improving security posture and enabling seamless identity federation across platforms. Implemented comprehensive IAM solution supporting 32,000+ global users with 40+ integrated applications.

PRIVILEGED ACCESS SECURITY TRANSFORMATION

LexisNexis & USPTO | 2024

- Spearheaded enterprise-wide privileged access security program incorporating modern PAM solutions, Just-In-Time access, behavioral analytics, and continuous monitoring. Implemented comprehensive secret management solution for applications and DevOps pipelines. Reduced privileged credential exposure by 90% while enabling automated auditing and compliance reporting. Solution became reference architecture for other federal agencies, cited as exemplary implementation of CISA Zero Trust maturity model.

EDUCATION

- **BACHELOR'S OF SCIENCE IN CYBERSECURITY,** 2025
[University of Richmond](#)
Relevant Coursework: Network Security, Cryptography, Ethical Hacking
- **ASSOCIATE OF APPLIED SCIENCE IN INFORMATION SYSTEMS,** 2021
[Reynolds College](#)
Relevant Coursework: Database Management, Web Development, Programming Fundamentals

CERTIFICATIONS

- **AZ-900,** Microsoft Azure Fundamentals 2025
- **Cybersecurity Essentials,** Cisco 2021
- **IBM Cloud Essentials,** IBM 2021
- **Network Administration,** Reynolds College 2020

AWARDS AND HONORS

- **Phi Theta Kappa Honor Society,** International Honor Society 2018
- **Dean's List,** Reynolds College 2018