RONNIE BAILEY

Richmond, VA | (804) 610-9719
opportunities@ronniebailey.cloud | www.linkedin.com/in/ronniebailey

Principal IAM Architect with 15 years architecting identity security for Fortune 500 enterprises and federal agencies. Expert in Zero Trust architecture, privileged access management, and hybrid identity infrastructure. Technical escalation authority who designs frameworks, mentors teams, and resolves complex authentication failures.

LEAD IDENTITY SECURITY ARCHITECT

LexisNexis, United States Patent and Trademark Office 09/2024 – Present

Public Trust Clearance (Previously held, clearable)

- Constructed Zero Trust framework with JIT provisioning and risk-based authentication aligned with NIST 800-207, implementing continuous authentication monitoring that dynamically adjusts access based on real-time risk signals derived from behavioral analytics.
- Applied MITRE ATT&CK framework to systematically evaluate organizational security posture, identifying which adversary tactics current controls effectively address versus areas requiring additional protection used structured approach to prioritize security investments and communicate risk gaps to leadership in business terms.
- Led Azure security blueprint development integrating NIST 800-53 and CIS frameworks with compliance validation and reporting workflows, implemented Infrastructure-as-Code security policies that automatically enforce baseline configurations and detect drift in real time.
- Implemented consistent security controls across AWS, Azure, and GCP with centralized CSPM integration and automated misconfiguration detection built unified security dashboards aggregating risk signals across cloud platforms for executive visibility.
- Communicated complex security architecture and data insights to technical teams and non-technical stakeholders, translating technical risk into business impact for executive decision-making, led proof-of-concept testing for emerging security automation technologies.
- Redesigned and operationalized One Identity Safeguard platform for enterprise-wide privileged access control across hybrid infrastructure, executed full offboarding and re-onboarding of privileged assets, ensuring secure session recording, account rotation, and access policy re-alignment.
- Engineered automated threat correlation across CrowdStrike Falcon, Microsoft Defender, Palo Alto, and Checkpoint platforms using MITRE ATT&CK framework, intelligent alert triage, deduplication, and orchestrated remediation workflows dramatically reduced incident response time.

- Utilized One Identity Safeguard, Secureworks Taegis, and Sophos MDR to monitor privileged sessions across 500+ hybrid systems behavioral analytics detect anomalous behavior and automatically trigger orchestrated containment workflows.
- Integrated Auth0 into enterprise IAM stack to enable OAuth2/OpenID Connect-based SSO across internal applications, supporting FedRAMP and NIST 800-53-compliant authentication workflows with automated certificate rotation and trust validation.
- Designed and executed forensic response plans using Secureworks Taegis, implementing NIST 800-86-aligned chain-of-custody workflows with automated evidence preservation and integrity validation.

IAM ARCHITECT

Kroger, Technology & Digital Department 12/2022 – 02/2024

- Led identity provisioning implementation for 32,000+ users across US/UK teams while maintaining HIPAA compliance built intelligent provisioning workflows that automatically adjust access based on role patterns and peer analysis.
- Implemented OneIdentity Safeguard/TPAM with automated just-in-time privilege elevation aligned with NIST 800-53, substantially reducing standing privileged access through ServiceNow integration that grants temporary elevated access based on approved change tickets.
- Engineered security modernization using Entra ID/Azure AD for 12,000+ hybrid users with Kubernetes service identity integration designed AKS pod identity solution that eliminated static credentials in containerized applications through workload identity federation.
- Integrated Ping SSO/MFA across 40+ applications with risk-based authentication policies that dynamically adjust verification requirements implemented behavioral analytics that significantly reduced password-reset tickets while cutting unauthorized access attempts.
- Implemented continuous access certification automation leveraging behavioral analytics to identify dormant accounts, excessive permissions, and separation-of-duties violations intelligent entitlement review workflows automatically recommend access revocations based on usage patterns.
- Deployed CrowdStrike Falcon with automated threat hunting playbooks across 2,000+ endpoints, substantially reducing malware incidents through proactive detection and orchestrated response capabilities.
- Standardized infrastructure using VMware vSphere across production and test environments with automated VM lifecycle management, improving system uptime while reducing operational costs through infrastructure-as-code provisioning.
- Engineered automated joiner/mover/leaver workflows with AI-driven anomaly detection for 20,000+ accounts implemented ML-based provisioning logic that identifies access anomalies and automatically triggers security reviews when patterns deviate from established baselines.
- Enhanced security with Varonis automated file access monitoring and data classification, improving audit readiness for SOX/GDPR compliance through continuous policy validation and automated remediation of excessive permissions.

- Streamlined Active Directory with automated RBAC/conditional access policies through continuous access validation and intelligent policy recommendations based on historical access patterns.

CUSTOMER IDENTITY & ACCESS MANAGEMENT ARCHITECT

Homeland Security, OCIO – US Secret Service | Contract 02/2022 – 12/2022

Public Trust Clearance (Previously held, clearable)

- Positioned IAM as a cornerstone of DHS security strategy, integrating Active Directory, OAuth 2.0, and SAML 2.0 authentication for 100+ legacy systems across distributed federal infrastructure with automated federation trust management.
- Spearheaded ISO 27001 certification for DHS Information Security Management System, establishing enterprise security governance framework with automated control validation adopted agency-wide.
- Orchestrated GCP migration for 50+ on-premises systems, enabling FedRAMP Moderate authorization with comprehensive SIEM integration and automated continuous compliance monitoring,implemented infrastructure-as-code security baselines ensuring consistent configuration.
- Implemented secure identity practices for serverless functions in GCP with automated workload identity federation, enabling principle of least privilege with function-level permissions that dynamically adjust based on runtime context.
- Enforced granular access policies via Saviynt across 15,000+ user accounts with automated entitlement reviews and separation-of-duties enforcement, dramatically reducing manual certification effort through intelligent access analytics.
- Utilized Agile/SCRUM methodologies with scripting (PowerShell, Python, Java) to enhance system resilience and efficiency in alignment with FISMA compliance, building reusable automation modules adopted across DHS security teams.

CLOUD VULNERABILITY ANALYST

Accessia Health | Contract 07/2021 – 12/2021

- Led vulnerability assessments aligned with NIST 800-53 and HIPAA standards using automated scanning and intelligent risk prioritization based on exploitability, business criticality, and threat intelligence.
- Implemented compliance reporting via PingFederate logs for SOX, GDPR, and HIPAA audits, streamlining evidence collection and regulatory reporting, built real-time compliance dashboards providing continuous visibility into authentication security posture.
- Deployed PingFederate and Citrix NetScaler achieving high availability for mission-critical healthcare applications through automated failover and health monitoring.
- Spearheaded automated credential vaulting and rotation for privileged accounts across healthcare systems, eliminating static privileged credentials.
- Implemented identity-aware proxies and service meshes for securing microservices architecture in AWS with automated policy enforcement, enabling zero trust network access for containerized healthcare applications.

- Reviewed infrastructure changes and provided automated security feedback using policy-as-code frameworks to ensure compliance with cloud security standards before deployment.
- Modernized SSL/TLS protocols for 150+ domains with automated certificate lifecycle management, maintaining full compliance with healthcare security requirements while eliminating manual certificate tracking.

PRIVILEGED ACCESS MANAGEMENT ARCHITECT

Indivior Pharmaceuticals 10/2019 – 07/2021

- Mapped 200+ job functions to least privilege roles using automated RBAC analysis, substantially reducing excessive permissions across enterprise applications through systematic role optimization.
- Briefed executive leadership regularly on security risks, compliance gaps, and mitigation strategies across AWS environments, translated technical findings to business impact with data driven risk dashboards informing strategic security investments.
- Deployed BeyondTrust PAM securing 1,200+ privileged accounts with SOX compliant audit controls and automated credential rotation policies, eliminating standing privileged access for routine operations.
- Architectural role based, location-based, and device compliance policies in Microsoft Entra ID with automated risk scoring that dynamically enforces access controls based on real-time threat intelligence and user behavior patterns.
- Designed GCP security framework using Google IAM and Security Command Center with automated real-time threat detection and policy enforcement across cloud workloads, integrating with central SIEM for unified security monitoring.
- Integrated Azure AD/Entra ID with intelligent authentication that adapts verification requirements based on risk signals, enhancing user verification while streamlining access management.
- Implemented BitLocker encryption with automated deployment and backup policies to safeguard ePHI across all endpoints in compliance with HIPAA requirements.
- Implemented risk-based authentication with context aware access policies that dynamically adjust security requirements based on user behavior, device posture, and threat intelligence.
- Integrated security guardrails into Terraform deployments using automated policy validation, ensuring compliance from deployment to runtime through continuous security scanning and drift detection.
- Designed IAM solutions using Microsoft Intune with automated mobile device management and remote access enforcement for distributed workforce.
- Maintained Carbon Black with automated threat hunting playbooks, policy enforcement, and orchestrated incident response across enterprise endpoints.

IDENTITY AND ACCESS MANAGEMENT ANALYST

Wells Fargo | Contract 04/2019 – 10/2019

- Designed Zero Trust aligned IAM framework with automated risk based access controls through continuous verification and intelligent policy recommendations based on access patterns.
- Implemented consistent identity controls across AWS and Azure environments with automated policy synchronization through infrastructure-as-code automation.
- Enforced FFIEC and GLBA requirements via SCCM and Office 365 with automated access controls and continuous compliance monitoring.
- Leveraged Microsoft Defender's automated remediation capabilities through orchestrated threat response workflows and intelligent alert correlation.
- Engineered progressive profiling workflows using ADFS with automated failover for customer-facing banking applications, implementing intelligent session management and fraud detection.
- Maintained 12,000+ user accounts across hybrid environments through automated lifecycle workflows with intelligent provisioning ensuring timely access grants and revocations based on HR system integration.
- Conducted staff security education while implementing automated phishing response workflows, substantially reducing incident response time through orchestrated investigation and remediation.
- Briefed upper management on cloud security risks and mitigation strategies with automated risk dashboards providing actionable recommendations and continuous visibility into security posture trends.

CUSTOMER IDENTITY & ACCESS MANAGEMENT ENGINEER

Wellsecured IT 10/2015 – 01/2019

- Designed and implemented unified Zero Trust frameworks across Azure, GCP, and M365, aligning conditional access, PIM, and JIT workflows to reduce standing privileges by over 70% while strengthening organizational security posture.
- Served as technical escalation for business critical IAM failures including certificate expirations, broken SAML trusts, and provisioning system outages, primary authority for resolving complex authentication issues when automated remediation and support tiers cannot resolve.
- Mentored IAM engineers on automation frameworks, schema change management, and certificate lifecycle operations, created standardized operational runbooks and automation templates that reduced team dependency on senior resources.
- Engineered automated certificate monitoring and renewal systems for SAML, OIDC, and OAuth2 across 100+ enterprise applications, proactive 60 day alerts and coordination with SaaS vendors eliminated authentication outages and manual tracking overhead.
- Managed directory schema and attribute governance across Entra ID, Active Directory, and ActiveIDM, ensuring data integrity in automated user lifecycle processes, eliminated sync failures between Workday, AD, and downstream identity repositories through intelligent data validation.

- Primary escalation point for Workday-to-AD-to-Entra provisioning workflows, resolving complex attribute mapping failures and sync errors that blocked automated joiner/mover/leaver processes across hybrid identity stack.
- Administered ActiveIDM's role-based provisioning engine with intelligent exception handling that automatically routes edge cases to appropriate approvers based on organizational hierarchy and risk level.
- Led migration to ForgeRock Identity Management with automated workflow standardization for hybrid environments, substantially reducing provisioning delays through intelligent lifecycle automation and exception handling.
- Integrated Splunk with IAM tools for automated security event monitoring and alerting, achieving ISO/IEC 27001 and NIST 800-53 compliance through centralized log correlation and intelligent threat detection.
- Spearheaded Auth0 integration for client facing portals with intelligent authentication that balanced security requirements with user experience for financial services clients.
- Generated conditional access policies using Microsoft Defender with automated policy recommendations for privileged account management, enforcing risk-based access decisions through continuous policy evaluation.
- Implemented OAuth 2.0 and OpenID Connect protocols with automated token lifecycle management for securing cloud-native application APIs and microservices architectures.
- Built AWS IAM roles and encryption protocols across multi-cloud environments with automated policy enforcement ensuring consistent least-privilege access patterns.
- Partnered with DevOps teams to implement automated log analysis and incident response through CI/CD pipeline integration.

CLOUD SECURITY OPERATIONS LEAD

Cloudcentria Security 06/2011 – 12/2015

- Developed NIST 800-53 and ISO 27001-aligned policies with automated continuous validation, establishing security governance framework with policy-as-code implementation adopted organization-wide.
- Led investigation recovering stolen intellectual property with automated evidence collection and chain-of-custody workflows, establishing cloud forensics protocols that became industry standard practice.
- Implemented comprehensive automated security for IaaS, PaaS, and serverless deployments across AWS environments with continuous security validation.
- Scaled Nessus-based assessments to 15,000+ assets in AWS/Azure infrastructure with automated vulnerability prioritization based on exploitability and business impact.
- Integrated Ping Identity with Okta across SaaS platforms using automated federation trust management, substantially reducing helpdesk authentication requests and improving user experience.
- Maintained SAML, OIDC, and OAuth2 federation infrastructure while coordinating directly with SaaS vendors (Okta, Auth0, application providers) to debug authentication issues, resolve metadata exchange failures, and restore broken authentication flows.

- Optimized EntraID Connect sync logic and hybrid sync rules, normalizing attributes and UPN conventions to maintain consistent identity data across cloud and on-premises environments.
- Documented AD infrastructure including group memberships, OU design, and policy enforcement to support hybrid authentication and maintain authoritative identity sources.
- Administered BeyondTrust Password Safe with automated secret rotation and vault access workflows, eliminating credential sprawl through JIT automation tied to approved change management processes.
- Partnered with application teams to onboard enterprise apps to Entra ID, built self-service portals with standardized integration patterns that significantly reduced IAM team involvement in routine onboarding.
- Collaborated with SOC during security incidents, analyzing token misuse, privileged session activity, and authentication anomalies to support containment and forensic analysis.

SELECT CONSULTING ENGAGEMENTS

Short-term specialized implementations demonstrating rapid problem-solving across diverse industries

NUCLEAR ENERGY CLOUD IAM TRANSFORMATION 2024

Westinghouse Electric Company

- Designed and implemented federated identity architecture enabling secure nuclear data processing in the initial cloud environment.
- Built multi-factor authentication solution using Azure AD meeting nuclear industry security standards for the first phase of deployment.
- Implemented comprehensive Conditional Access policies covering all critical access scenarios for cloud resources.
- Worked directly with product owners to deploy Just-In-Time access through Privileged Identity Management for administrator accounts.
- Created and executed a thorough security testing protocol ensuring compliance with regulatory requirements for initial deployment.

MUNICIPAL IDENTITY THREAT PROTECTION 2024

City of Chesapeake, Virginia

- Integrated CrowdStrike Falcon with existing identity systems, establishing real-time monitoring of authentication activities.
- Implemented comprehensive Active Directory security controls, including tiered administrative model for privileged access.
- Developed a practical role-based access control framework for critical municipal systems, balancing security with operational needs.
- Created and delivered focused training sessions for IT staff on identity threat detection using real-world attack scenarios.

FEDERAL ICAM COMPLIANCE ANALYSIS 2023

Department of Veterans Affairs

- Conducted comprehensive analysis of privileged accounts across federal systems using CyberArk PAM to identify and categorize security gaps.
- Created automated reports that improved PIV compliance metrics by 35%.
- Designed integration approach between SailPoint and OKTA platforms, establishing foundation for streamlined identity governance.
- Implemented CyberArk policies aligned with Azure AD Conditional Access rules, enhancing security while maintaining operational efficiency.
- Established centralized logging for key identity events via Azure Event Hub, creating a unified view of authentication activities.

ENTERPRISE PROVISIONING AUTOMATION 2022

Lithia Motors

- Created custom Azure Log Analytics workspaces to monitor critical provisioning workflows, giving real-time visibility into account creation.
- Implemented standardized workflows between US and UK IT teams, establishing consistent provisioning practices across regions.
- Remediated key technical debt issues from legacy provisioning practices and implemented Defender EDR policies that improved security posture.
- Built automated compliance reporting using KQL queries against Azure Sentinel data, providing leadership with actionable metrics.

RETAIL AUTHENTICATION DIRECTORY 2021

Lands' End

- Designed and implemented specialized authentication directory with selective attribute filtering for secure external partner access.
- Built PingFederate authentication policies with core MFA capabilities that balanced security requirements with usability.
- Implemented essential OpenID Connect components for customer-facing applications, enhancing digital shopping experience.
- Articulated practical security recommendations that aligned IAM strategy with business objectives for leadership approval.
- Created integrated troubleshooting tools for helpdesk with ServiceNow ITSM integration, reducing resolution time for common issues.

EDUCATION

- **Bachelor of Science in Cybersecurity** | In Progress | University of Richmond
- **Associate of Applied Science in Information Systems** | Reynolds College