RONNIE BAILEY

RICHMOND, VA | (360) 719-8377

[career@ronniebailey.cloud](http://career@ronniebailey.cloud) | [linkedin.com/in/ronniebailey](https://www.linkedin.com/in/ronnie-bailey-7258a074)

**ABOUT ME**

Highly experienced Senior Cloud Security professional with a proven track record of success in delivering cloud-based security solutions that effectively meet operational and compliance requirements. With over a decade of expertise, I possess a deep understanding of the intricacies of cloud security and possess the ability to ensure stakeholders' needs are met while maintaining robust security measures.

**EXPERIENCE**

| • Access Control/Change Management | • ISO/ NERC CIP/ NIST/ SEC 501 |
| --- | --- |
| • Active Directory/GPO Administration | • Linux Mainframe Environment |
| • Amazon Web Service | • Jira |
| • API Management/Apigee | • Microsoft 365 |
| • Auth0 | • Microsoft Intune |
| • Azure AD | • Mobile Device Management (MDM) |
| • Bomgar/BeyondTrust | • OAuth, OIDC, SAML, SSO |
| • Cisco Meraki | • OneIdentity Safeguard |
| • Citrix Remote Desktop | • Password Management |
| • Confluence | • PingFederate |
| • Crowdstrike | • Powershell Scripting, Python |
| • Data Classification | • Qradar |
| • Documentation | • Rapid7 |
| • Fortinet Suite | • REST API/ JSON/ JavaScript |
| • Github | • RSA MFA |
| • HIPAA, NIST Frameworks | • Security Identity Manager (IBM) |
| • HRIS/ UltiPro/ Workday | • ServiceNow |
| • Hybrid Migration, On-Prem to Cloud | • Varonis |
| • Identity Solutions Design &  Implementation | • Windows Server Administration |
|  |  |

**CAREER**

**CUSTOMER IDENTITY & ACCESS MANAGEMENT, ARCHITECT SME**

**3/2022 – PRESENT | D.H.S., U.S. SECRET SERVICE**

* Performs IAM architect duties, developing and implementing IAM solutions, improving system architecture, and designing Cloud Identity Management solutions with Zero Trust methodologies.
* Designing and implementing CIAM solutions using Okta's Identity and Access Management platform.
* Manages DHS enterprise network security program, promotes IAM governance, and utilizes scripting knowledge.
* Proficient in configuring and customizing Okta's features, including user lifecycle management, single sign-on (SSO), multi-factor authentication (MFA), and API integration.
* Collaborates with IT and business leaders to implement layered security controls and scalable information security solutions based on business requirements.
* Monitors system performance and utilization metrics, documents IAM applications architecture, and resolves potential issues effectively.
* Leads project in transitioning IT governance framework from on-prem to cloud environment, generates roadmaps, and establishes procedures for user access, access controls, and administrative practices in IAM solutions.
* Demonstrates expertise in integrating Okta with various enterprise applications, such as cloud-based SaaS solutions, on-premises systems, and mobile applications.

**SR. CUSTOMER IDENTITY AND ACCESS MANAGEMENT (CIAM), ENGINEER  
12/2021 – 12/2022** | **LANDS’ END**

* Implemented OpenID Connect, OAuth 2.0, SSO, and MFA.
* Articulated cybersecurity architecture vision and strategies to guide leadership decision-making.
* Provided end-to-end support for Identity and Access Management lifecycle including on/off-boarding, conversions, transfers, IAM compliance, and role management.
* Designed, implemented, supported, and maintained PingIdentity SSO platform.
* Managed domain object lifecycles through automation and integration with key systems.
* Participated in software development in Java, SQL, and JavaScript.
* Experienced in security protocols such as LDAP-S, SAML, WS-Federation, SCIM, OAuth, and OIDC.

**SECURITY NETWORK ENGINEER  
7/2021 – 12/2021 | ACCESSIA HEALTH**

* Maintained server compliance with the ACF2 environment through Unix scripting.
* Ensured continuous functioning of system interfaces/connectors and coordinated with IT for technical support.
* Enforced SP 1800-30 guidelines to protect confidential data in healthcare applications and general Internet access.
* Created IT and business documentation for internal processes and procedures.

**IDENTITY AND ACCESS MANAGEMENT, ADMINISTRATOR  
10/2019 – 7/2021 | INDIVIOR PHARMACEUTICALS**

* Ensured ePHI data protection and encryption through off-site backups and Microsoft Bitlocker.
* Investigated threats, managed HBSS policies using Ivanti, and performed compliance scans using Microsoft Intune, Azure AD Services, and Defender.
* Managed user account profiles in Active Directory and Exchange Server for access control and security.
* Configured and authenticated Microsoft Defender for Exchange and Office 365 email security.
* Administered hybrid Identity and Access Management to mitigate identity-related risks.

**IDENTITY & ACCESS MANAGEMENT, SR. ANALYST  
4/2019 – 10/2019 | WELLS FARGO**

* Established and maintained user accounts, profiles, network and system security, and access privileges through IAM tools such as Active Directory, Office 365, and SCCM.
* Designed plans for future systems and infrastructure strategies, including Windows 10 and Azure AD migrations and Mobile Device Management solutions.
* Conducted on and off-boarding and trained 400 employees on security processes, reducing phishing attacks.
* Improved IT department effectiveness by 35% with SCCM tools for monitoring and preventative maintenance.
* Ensured IAM practices were compliant with the bank's operational risk framework and industry best practices, including policies, procedures, and control methodologies.
* Managed phishing simulation campaigns and provided system and network administration support.
* Worked with software and hardware vendors to document changes for troubleshooting and remediation.

**IDENTITY AND ACCESS MANAGEMENT, ANALYST  
10/2015 – 1/2019 | WELLSECURED IT**

* Created and maintained documentation of the IT Risk program and any exceptions for regulatory compliance.
* Performed implementation, upgrade and testing tasks for systems and network security technologies through utilization of change control methodologies.
* Installed virtual machines (VMWare, VirtualBox, & Hyper-V) to utilize applications in a test environment.
* Provided complex technical guidance, oversight, and enforcement of security directives, policies, standards, plans, and procedures as defined by ISO/IEC 27001 framework.
* Defined and documented IT security requirements and communicated through effective security programs and training.
* Compiled and documented data in support of equipment and/or user changes of system migrations.

**IDENTITY & ACCESS MANAGEMENT, SOLUTIONS ENGINEER  
6/2011 – 3/2022 | CLOUDCENTRIA SECURITY**

* Directed, coordinated, and controlled services to ensure alignment with business direction and compliance with standards, policies, and budgets.
* Communicated company wide architecture strategy and direction to management and systems teams.
* Supported the Identity and Access Management group, providing strategic guidance and collaborating on design and implementation projects.
* Created artifacts such as position papers, blueprints, and reference architectures.
* Led architectural support for product and vendor evaluations addressing IAM functionality and security threats.
* Provided oversight and technical leadership across all cybersecurity domains to ensure system confidentiality, integrity, and availability.

**EDUCATION  
 BACHELOR OF SCIENCE IN CYBERSECURITY,** 5/2023 | UNIVERSITY OF RICHMOND | RICHMOND, VA **ASSOCIATE OF APPLIED SCIENCE IN INFORMATION SYSTEMS,** 8/2020 | REYNOLDS COLLEGE | RICHMOND, VA

**CERTIFICATION  
 AZ-900, MICROSOFT AZURE,** 12/2023 | IN PROGRESS **CYBERSECURITY ESSENTIALS,** 10/2021 | CISCO NETWORKING ACADEMY  
 **NETWORK ADMINISTRATION,** 8/2021 | REYNOLDS COLLEGE