RONNIE BAILEY

RICHMOND, VA | (360) 719-8377

ronniebailey@live.com | linkedin.com/in/ronniebailey

Sr Cloud Security Principal Architect with over 10 years of experience specializing in designing, implementing, and managing cloud-based security solutions for a variety of industries.

TECHNICAL PROFICIENCIES

- **ACCESS MANAGEMENT:**
  Access Control / Change Management, Active Directory / GPO Administration,ForgeRock Identity Platform (Access Management, Identity Management, Directory Services, Identity Gateway), Identity Solutions Design & Implementation, Microsoft Intune, Mobile Device Management (MDM), OAuth, OIDC, SAML, SSO, OneIdentity Safeguard: Privileged Passwords, Password Management, and Total Privileged Access Management (TPAM)

- **CLOUD COMPUTING:**
  Amazon Web Services (AWS), Azure, Azure Active Directory / Entra ID, Google Portal, and Hybrid Migration, On-Prem to Cloud

- **DEVELOPMENT:**
  Agile Development, API Management / Apigee, Auth0, PowerShell Scripting, Python, and REST API / JSON / JavaScript.

- **FRAMEWORKS & COMPLIANCE:**
  Business Continuity Planning, Data Classification, Disaster Recovery, FISMA, HIPAA, HITRUST, ISO 27001, NIST Frameworks

- **NETWORKING & REMOTE ACCESS:**
  Bomgar/BeyondTrust, Cisco Meraki, Citrix Remote Desktop, Fortinet Suite, Ping Identity

- **SECURITY & VULNERABILITY MANAGEMENT:**
  Security Information and Event Management, Vulnerability Management

- **SOFTWARE & TOOLS:**
  Confluence, Crowdstrike, DevOps, Microsoft 365, QRadar, Rapid7, RSA / MFA, Security Identity Manager (IBM), ServiceNow, Varonis

- **SYSTEM ADMINISTRATION & MANAGEMENT:**
  IT Infrastructure Management,IT Service Management, Linux Mainframe Environment, Windows Server Administration

- **OTHER:**
  Agile Development, Digital Asset Management, Scrum, Waterfall, etc.

CAREER

SR. PRINCIPAL SECURITY ARCHITECT
D.H.S., U.S. Secret Service
3/2022 - Present

- Implements the design and implementation of a new IAM solution for the U.S. Secret Service, improving system architecture and security posture.
- Orchestrates cloud migration using Azure AD, ensuring secure and efficient transfer of critical systems from on-prem to cloud environments.
- Utilizes Agile development and scripting languages (PowerShell, Python) for system resilience and efficiency in accordance with the FISMA framework.
- Designs and implements identity solutions using Active Directory, OAuth, and SAML, emphasizing cloud security.
- Manages the DHS enterprise network security program, promoting IAM governance and utilizing scripting knowledge.
- Monitored server and firewall logs, analyzed network traffic, and conducted regular vulnerability scans using tools like Qualys to maintain robust security.
- Investigated and resolved complex security breaches and vulnerability issues with a strong emphasis on accuracy and timeliness, while conducting user activity audits using IAM tools like Active Directory.

SR. PRIVILEGE ACCESS MANAGEMENT (PAM), ENGINEER
Lands' End
12/2021 - 12/2022

- Deployed OneIdentity Safeguard for robust privileged password management, integrating it with existing systems for streamlined access control.
- Designed, implemented, supported, and maintained the PingIdentity SSO platform,OpenID Connect, OAuth 2.0, and MFA.
- Conducted regular audits and adjustments of privileged access settings, leveraging OneIdentity's analytics to enhance system security.
- Drove Total Privileged Access Management (TPAM) initiatives for robust security frameworks.
- Articulated cybersecurity architecture vision and strategies to guide leadership decision-making.
- Provided end-to-end support for the Identity and Access Management lifecycle, including on/off-boarding, conversions, transfers, IAM compliance, and role management.
- Experienced in security protocols such as LDAP-S, SAML, WS-Federation, SCIM, OAuth, and OIDC.
- Evaluated existing security technologies and recommended the adoption of new and emerging IAM solutions, such as Auth0, to enhance the organization's security posture.
- Effectively communicated critical updates to key stakeholders throughout the organization, utilizing collaboration tools like Confluence.

INFOSEC ADMINISTRATOR

Accessia Health

7/2021 - 12/2021

- Managed vulnerability assessments, remediation strategies, and ensured HIPAA and NIST compliance.
- Enforced SP 1800-30 guidelines to protect confidential data in healthcare applications and general Internet access.
- Conducted system audits and policy enforcement for robust security compliance.
- Regularly updated security protocols in alignment with the latest QRadar documentation, ensuring optimal configuration for threat detection.
- Maintained server compliance with the ACF2 environment through Unix scripting.
- Ensured continuous functioning of system interfaces/connectors, coordinated with IT.

IDENTITY AND ACCESS MANAGEMENT (IAM), PRINCIPAL ENGINEER

Indivior Pharmaceuticals

10/2019 - 7/2021

- Integrated SSO and MFA using Microsoft Azure Active Directory, enhancing user verification processes and access management.
- Ensured ePHI data protection and encryption through off-site backups and Microsoft Bitlocker.
- Designed IAM solutions using Microsoft Intune for efficient mobile device management, ensuring secure and remote access.
- Managed user account profiles in Active Directory and Exchange Server for access control and security.
- Investigated threats, managed HBSS policies using Ivanti, and performed compliance scans using Microsoft Intune, Azure AD Services, and Defender.

IDENTITY AND ACCESS MANAGEMENT (IAM), ANALYST

Wells Fargo

4/2019 - 10/2019

- Ensured IAM practices were compliant with the bank's operational risk framework and industry best practices, including policies, procedures, and control methodologies.
- Managed and configured user roles and permissions in Active Directory, utilizing GPOs for enforcing security policies across the network.
- Established and maintained user accounts, profiles, network and system security, and access privileges through IAM tools such as Active Directory, Office 365, and SCCM.
- Supported IAM solutions design and maintenance, focusing on access control systems.
- 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.

CUSTOMER IDENTITY AND ACCESS MANAGEMENT (CIAM) ENGINEER

Wellsecured IT
10/2015 - 1/2019

- Orchestrated the migration of legacy IAM systems to ForgeRock IDM, improving identity lifecycle management and reducing operational costs.
- Implemented CIAM solutions focusing on enhancing user experience, utilizing analytics to tailor access management to customer needs.
- Provided complex technical guidance, oversight, and enforcement of security directives, policies, standards, plans, and procedures as defined by ISO/IEC 27001 framework.
- Created and maintained documentation of the IT Risk program and any exceptions for regulatory compliance.
- Defined and documented IT security requirements and communicated through effective security programs and training.
- Created industry leading practices of Identity and Access Management/Access Control/Change Management through Active Directory and Azure AD PaaS.
- Installed virtual machines (VMWare, VirtualBox, & Hyper-V) to utilize applications in a test environment.

CLOUD SECURITY OPERATIONS

Cloudcentria Security
6/2011 - 12/2015

- Developed and maintained policies, procedures, and documentation to align with regulatory standards, leading to successful audits and certifications.
- Collaborated cross-functionally with IT, legal, and business teams to design and implement effective risk mitigation strategies.
- Monitored Azure environment using cloud-specific security tools, implementing custom security measures based on vendor guidelines.
- Implemented automated GRC tools, streamlining risk assessment processes and reducing manual workload by 30%.

SYSTEM ADMINISTRATOR

uBreakiFix
6/2009 - 12/2011

- Provided first-level technical support to end-users via phone, email, or in-person, addressing issues with hardware and software, and network connectivity.
- Evaluated and prioritized incidents based on impact and urgency, contributing to meeting established service level agreements (SLAs).
- Maintained high-level customer satisfaction by delivering professional and timely support, and documenting processes and service desk records meticulously.

IT SUPPORT ASSOCIATE
Circuit City
9/2006 - 1/2009
- Provided comprehensive customer service, assisting with inquiries and resolving technical issues related to a wide range of electronic and computer products.
- Skilled in diagnosing and troubleshooting diverse hardware and software problems, ensuring customer satisfaction and repeat business.
- Conducted detailed product demonstrations, explaining complex technology in an accessible manner to enhance customer understanding and engagement.

EDUCATION

- Bachelor of Science in Cybersecurity, University of Richmond (Expected 2024)
- Associate of Applied Science in Information Systems, Reynolds College (2020)

CERTIFICATIONS

- **AZ-900**: Microsoft Azure Fundamentals (In progress)
- **Cybersecurity Essentials,** Cisco Networking Academy
- **Network Administration,** Reynolds College

AWARDS AND HONORS

- Phi Theta Kappa Honor Society, international honor society
- President's List, Reynolds College