

# RONNIE BAILEY

Richmond, VA // (360) 719-8377

[opportunities@ronniebailey.cloud](mailto:opportunities@ronniebailey.cloud) // [linkedin.com/in/ronniebailey](https://linkedin.com/in/ronniebailey)

Principal Identity Security professional with over a decade of experience in the cybersecurity industry. Specialized in IAM and Cloud Security. Known for effectively managing security solutions, leading to significant improvements in system security.

## PROFESSIONAL EXPERIENCE

### SECURITY AUTOMATION ENGINEER

04/2024 - Present

Lexis Nexus / United States Department of Patents and Trade

*\*Public Trust Clearance*

- Implements and manages IAM solutions using Azure AD, Active Directory, Entra ID, and RSA to establish robust identity and access management protocols.
- Deploys CrowdStrike Falcon for advanced threat detection and response, and incorporates SSO and MFA across the enterprise for enhanced security.
- Architects and integrates Zero Trust principles into the existing security infrastructure, focusing on least privilege and role-based access controls.
- Leads the migration from legacy IAM products to modern solutions such as the Microsoft Identity Platform and Okta, ensuring a seamless transition.
- Creates and maintains automation scripts using Bash, PowerShell, and Python, resulting in improved process efficiency and reliability.
- Engineers end-to-end IAM process flows and implements secure, role-based access management.
- Administers and troubleshoots Windows and Linux/Unix servers, ensuring optimal performance and stability.
- Manages PKI and Certificate Authorities, including Microsoft Windows Certificate Services, to secure communications and authentication.
- Implements NIST and ISO security standards in all IAM solutions, ensuring compliance and enhanced security posture.
- Mentors junior engineers, leads security initiatives, and manages projects to ensure successful and timely delivery.
- Produces clear technical documentation and effectively communicates complex technical information to diverse audiences.

## **PRINCIPAL SECURITY ARCHITECT, CYBERSECURITY**

12/2022 - 02/2024

Kroger, Technology & Digital Department

- Enhanced organizational security posture and compliance by leveraging Microsoft Azure AD/Entra ID for cloud services, Onedidentity Safeguard and TPAM for IAM, ensuring scalable and secure cloud infrastructure.
- Reduced system vulnerabilities and improved threat detection and response through the integration of CrowdStrike, focusing on advanced endpoint security.
- Drove the adoption of SailPoint, resulting in a 45% improvement in audit performance and a 35% reduction in unauthorized access through refined identity governance and automated provisioning processes.
- Streamlined user access control and enterprise management with Active Directory and LDAP, facilitating secure and efficient authentication processes.
- Integrated Okta to provide seamless identity and access management across cloud and on-premise applications, reinforcing the security framework.
- Protected sensitive information, ensuring regulatory compliance, by employing Varonis for threat detection and vulnerability management for data analytics.
- Supported secure collaboration and information sharing using Confluence, SharePoint, and Microsoft 365, incorporating security measures into business operations for devops and system automation.
- Managed and secured privileged passwords with One Identity's Privileged Password Management PPM, addressing access-related vulnerabilities.
- Oversaw security projects and initiatives, utilizing Jira with DevOps & security automation for effective tracking and execution, ensuring timely completion of security priorities.
- Created a comprehensive incident response plan for IAM breaches in the Citrix environment, detailing steps for detection, containment, and recovery.
- Orchestrated rollout of CrowdStrike Falcon to 10,000 endpoints for automated threat detection and response.

## **CUSTOMER IDENTITY & ACCESS MANAGEMENT**

02/2022 - 12/2022

Department of Homeland Security, OCIO, United States Secret Service,

*\*Public Trust Clearance*

- Streamlined CyberArk's Privileged Access Management system boosting audit compliance by 50% and cutting response times by 40% through implementing advanced security protocols and integrating automated threat detection features.
- Orchestrated cloud migration using GCP, ensuring secure and efficient transfer of critical systems from on-prem to cloud environments.
- Utilized Agile, SCRUM, and scripting languages including PowerShell, Python, and Java for system resilience and efficiency in accordance with the FISMA framework to meet compliance and security frameworks.

- Designed and implemented identity solutions using Active Directory, OAuth, and SAML emphasizing cloud security.
- Leveraged Fortinet in the transition to a zero-trust network architecture, significantly minimizing potential attack vectors enhancing security posture.
- Orchestrated the organization's successful FedRAMP authorization process, enabling secure and compliant cloud service offerings to federal agencies.
- Designed and implemented an information security management system (ISMS) that achieved ISO 27001 certification, significantly improving the organization's security posture and client confidence for the customer.
- Developed and enforced access policies using Saviynt's policy engine, leading to a 50% reduction in unauthorized access incidents.
- Utilized capabilities in Python and Powershell scripting for automation of security tasks, analysis, and tool development for GCP to create security solutions.
- Managed enterprise network security program, promoting IAM governance and utilizing scripting knowledge for IT infrastructure and operations management.
- Monitored server and firewall logs, analyzed network traffic, and conducted regular vulnerability scans using tools like Qualys for threat detection and vulnerability management to maintain robust security for the customer.
- Implemented robust incident response protocols using Fortinet solutions with GCP, reducing detection and response times for cybersecurity incidents.

## **CLOUD VULNERABILITY ANALYST**

07/2021 - 12/2021

### Accessia Health

- Managed vulnerability assessments, remediation strategies, and ensured HIPAA and NIST compliance.
- Configured Citrix NetScaler to integrate with PingAccess for enhanced secure access management, providing granular access controls for remote users.
- Developed training programs on the use of DICOM standards for imaging data, HL7 for electronic health information exchange, and IHE protocols to ensure interoperable use of healthcare information.
- Implemented PingFederate for single sign-on (SSO) across all Citrix-hosted applications, ensuring seamless user authentication and improved security.
- Designed and deployed multi-factor authentication using Microsoft
- Defender, reducing unauthorized access incidents by 75% within the first year of implementation.
- Generated monthly compliance reports from PingFederate logs, ensuring all IAM activities within the VDI environment met regulatory requirements.
- Directed the organization-wide SSL/TLS certificate management program, ensuring encryption standards compliance and preventing downtime due to expired certificates.<sup>3</sup>

- Directed the collection, analysis, and reporting of healthcare metrics, utilizing data from EHR and PACS systems to drive improvements in patient health outcomes and service delivery.
- Implemented Auth0 for secure, scalable user authentication, leading to a 99% success rate in logins and halving the development time for new auth features by leveraging customizable workflows and SDKs aligning with HIPPA requirements.
- Coordinated with IT, audit, and compliance teams to ensure CyberArk practices aligned with regulatory requirements, significantly contributing to successful audits under standards such as SOX, GDPR, and HIPAA.

## **PRIVILEGED ACCESS MANAGEMENT ARCHITECT**

10/2019 - 07/2021

Indivior Pharmaceuticals

- Integrated SSO and MFA using Microsoft Azure Active Directory/Entra ID enhancing user verification processes and access management.
- Ensured ePHI data protection and encryption through backups and Bitlocker.
- Designed IAM solutions using Microsoft Intune for efficient mobile device management, ensuring secure and remote access.
- Developed a centralized incident response management system on GitHub.
- Managed user account profiles in Active Directory and Linux Server for access control and security management.
- Orchestrated the selection, implementation, and optimization of healthcare technology systems, including advanced Electronic Health Records (EHR) platforms like Epic, to bolster patient care and clinical operations.
- Spearheaded the migration of identity governance to the cloud with SailPoint IdentityNow, facilitating secure and scalable access management for a distributed workforce.
- Collaborated with IT and security teams to define and map out roles based on job functions, ensuring minimum necessary access rights for over 500 users across various departments.
- Designed a secure GCP architecture using Google IAM and Security Command Center for cloud resource protection.
- Maintained optimized scripts, documented processes, trained staff, significantly improving operational resilience and team autonomy with scripting automation.
- Led the deployment of BeyondTrust to secure privileged accounts, reducing unauthorized access by 75% and enhancing compliance by 80% through strategic account management and audit controls.
- Maintained Carbon Black as comprehensive endpoint security from threat hunting to incident response.

- Designed and executed automated provisioning and deprovisioning processes in SailPoint, reducing manual workload by 70% and improving onboarding/offboarding efficiency.
- Designed role-based, location-based, & device compliance access controls for Entra ID.

## **IDENTITY AND ACCESS MANAGEMENT ANALYST**

04/2019 - 10/2019

Wells Fargo

- Ensured IAM practices were compliant with the bank's operational risk framework and industry best practices, including policies, procedures, and control methodologies.
- Led cybersecurity projects using Agile and Waterfall methodologies, improving team efficiency and adaptability to rapidly changing security threats.
- Maintained user accounts, profiles, network, system security, and access privileges through IAM tools such as Active Directory, Office 365, and SCCM.
- Supported IAM solutions and maintenance, focused on access control systems.
- Oversaw the migration of critical workloads to a vSphere-based virtualized infrastructure, resulting in improved resource utilization and a 20% reduction in data center costs.
- Utilized Microsoft Defender's automated investigation and remediation features to streamline security operations, achieving a 30% reduction in manual security tasks through automation.
- Developed and implemented advanced Splunk dashboards for comprehensive visibility into network traffic, system logs, and user activities, enhancing the security team's analytical capabilities, aiding in proactive threat hunting efforts.
- Utilized COBOL for system updates, bug fixes, and implementing new features to improve efficiency and reliability.
- Participated in cross-departmental projects to extend the functionality of COBOL applications, enabling new banking services and improving customer experience.
- Conducted on/off-boarding and trained 400 employees on security processes, reducing phishing attacks by presenting security awareness and training.

## **CUSTOMER IDENTITY & ACCESS MANAGEMENT ENGINEER**

10/2015 - 01/2019

Wellsecured IT

- Orchestrated the migration of legacy IAM systems to ForgeRock IDM, improving identity lifecycle management and reducing operational costs.
- Integrated Splunk with IAM solutions to automate the collection and analysis of access logs, streamlining audit processes and significantly improving the efficiency of compliance reporting.

- Provided complex technical guidance, oversight, and enforcement of security directives, policies, standards, plans, and procedures as defined by ISO/IEC 27001 framework.
- Ensured alignment with NIST and ISO 27001 standards by leveraging Microsoft Defender's security controls to protect sensitive data and maintain high compliance levels.
- Conducted comprehensive security audits using Ping Identity tools to identify and remediate potential vulnerabilities in the IAM infrastructure.
- Optimized application delivery and performance using Citrix, achieving a 99.9% uptime for critical applications and enhancing user satisfaction.
- Installed virtual machines (VMWare, VirtualBox, & Hyper-V) to utilize applications in a test environment of IT Infrastructure and operations management.
- Designed and deployed a suite of PowerShell scripts for automating security tasks, including log analysis, system hardening, and incident detection.
- Integrated a secure, scalable AWS cloud infrastructure with enhanced identity/access management and encryption, boosting efficiency and security.
- Integrated Auth0 for scalable user authentication, enhancing authentication success to 99% and cutting development time by 50% by adopting secure and efficient authentication workflows.

## **CLOUD SECURITY OPERATIONS**

06/2011 - 12/2015

### Cloudcentria Security

- Developed and maintained policies, procedures, and documentation to align with regulatory standards, leading to successful audits and certifications.
- Conducted penetration testing and vulnerability assessments using Kali Linux, identifying critical security weaknesses and recommending mitigation strategies to enhance system resilience.
- Led the integration of Ping Identity with enterprise applications, ensuring secure and efficient user access control to reduce administrative overhead.
- Maintained high-level customer satisfaction by delivering professional and timely support, and documenting processes and service desk records meticulously.
- Created industry leading practices of IAM/Access Control/Change Management through Active Directory and Azure AD/Entra ID PaaS.
- Spearheaded mitigation of sophisticated DDoS attacks, improving organizational threat resilience.
- Directed an enterprise-wide vulnerability management program using Nessus, covering 15,000 assets.
- Conducted a digital forensics investigation of a suspected insider threat, using The Sleuth Kit for disk image analysis and evidence recovery.

- Identified the malicious insider, leading to legal action and the recovery of stolen intellectual property.
- Developed best practices for forensic investigations, significantly improving incident response capabilities.

## EDUCATION

- **Bachelor's of Science in Cybersecurity,** 03/2025  
[University of Richmond](#)  
**Relevant Coursework:** Network Security, Cryptography, Ethical Hacking
- **Associate of Applied Science in Information Systems,** 05/2021  
[Reynolds College](#)  
**Relevant Coursework:** Database Management, Web Development, Programming Fundamentals

## CERTIFICATIONS

- **AZ-900,** Microsoft Azure Fundamentals 03/2025
- **Cybersecurity Essentials,** Cisco 10/2021
- **IBM Cloud Essentials,** IBM 10/2021
- **Network Administration,** Reynolds College 07/2020

## AWARDS AND HONORS

- **Phi Theta Kappa Honor Society,** International Honor Society 04/2018
- **Dean's List,** Reynolds College 06/2018