RONNIE BAILEY

Richmond, VA // (360) 719-8377
ronniebailey@live.com // linkedin.com/in/ronniebailey

Proven Principal Security Architect with 13+ years of experience designing, implementing, and managing comprehensive security solutions. Strong track record of building secure environments, mitigating risks, and ensuring regulatory adherence.

PROFESSIONAL EXPERIENCE

PRINCIPAL SECURITY ARCHITECT, CYBERSECURITY 12/2022 - 2/2024
Kroger, Technology & Digital Department

- Enhanced organizational security posture and compliance by leveraging Microsoft Azure AD/Entra ID for cloud services, OneIdentity 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.
- Orchestrated rollout of CrowdStrike Falcon to 10,000 endpoints for automated threat detection and response.

CUSTOMER IDENTITY & ACCESS MANAGEMENT ARCHITECT 02/2022 - 12/2022
Department of Homeland Security, OCIO, United States Secret Service

- 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 Azure AD/Entra ID, 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.
- 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, reducing detection and response times for cybersecurity incidents.
- Strong capabilities in Python and Powershell scripting for automation of security tasks, analysis, and tool development.

SR. PRINCIPAL PAM ARCHITECT 12/2021 - 12/2022
Lands’ End

- Led the strategic deployment of OneIdentity Safeguard, significantly enhancing privileged password management. This initiative was intricately integrated with our Active Directory environment, streamlining access control and security protocols within AD infrastructure.
- Designed and implemented a robust PingIdentity Single Sign-On (SSO) platform, integrating OpenID Connect, OAuth 2.0, and Multi-Factor Authentication (MFA)

within our AD framework. This ensured secure and efficient authentication processes for all AD accounts.
- Conducted detailed audits and adjustments of AD privileged access settings, leveraging OneIdentity analytics to strengthen the security posture of the AD environment and mitigate potential vulnerabilities.
- Directed a comprehensive enterprise migration to Azure AD, which not only optimized cloud identity and security services but also achieved a remarkable improvement in login efficiency by 40%. This migration halved identity-related incidents by leveraging SSO and syncing seamlessly with our existing AD infrastructure and operations management systems.
- Led the integration of Splunk with multiple data sources, including log files, APIs, and databases, enhancing the data analysis capabilities and providing a 360-degree view of the organization's operational health.
- Utilized Saviynt's Cloud PAM to manage, monitor, and control access to critical cloud resources within our AD landscape, significantly reducing the risk of unauthorized access and enhancing security.
- Utilized Splunk Enterprise Security for continuous monitoring and incident response, developing advanced correlation searches and alerts that reduced false positives by 40% and improved threat detection accuracy.
- Implemented IBM QRadar SIEM for advanced threat detection and security analytics, specifically focusing on reducing false positives by 50% and enhancing security incident response times within our AD domain.
- Conducted comprehensive audits and compliance checks, ensuring 100% adherence to industry standards and regulations, including SSL/TLS best practices and PKI governance.

CLOUD VULNERABILITY ANALYST 07/2021 - 12/2021

Accessia Health

- Managed vulnerability assessments, remediation strategies, and ensured HIPAA and NIST compliance.
- Integrated Okta Customer Identity Cloud into several front-end applications, enabling secure and user-friendly authentication and authorization features, which enhanced user engagement by 20%.
- Enforced SP 1800-30 guidelines to protect confidential data in healthcare applications and general Internet access and OpenID Connect.
- Implemented CrowdStrike Falcon, increasing threat detection by 95% and minimizing incident response time utilizing AI-based analysis and automated response capabilities.
- Collaborated with application development teams to integrate SSL/TLS certificates into new web apps, ensuring secure communications from the outset.

- Designed a cloud-native architecture leveraging Okta Customer Identity Cloud to ensure secure, scalable, and efficient management of customer identities across multiple cloud environments.
- Implemented a zero-trust security model using Okta to protect sensitive customer data across public and private cloud services, reducing security incidents.
- Regularly updated security protocols in alignment with the latest QRadar documentation, ensuring optimal configuration for threat detection management..
- Successfully implemented Okta for information security integrating key applications like Salesforce and Office 365. Achieved a 30% increase in login efficiency and reduced password support tickets, enhancing security and user experience.
- Directed the organization-wide SSL/TLS certificate management program, ensuring encryption standards compliance and preventing downtime due to expired certificates.
- Established and maintained a private Certificate Authority, enabling the issuance and management of digital certificates for internal servers and applications, enhancing the internal network's trust and security.
- Maintained server compliance with the ACF2 environment through Unix/Linux scripting and automation.
- Integrated ForgeRock with legacy systems and cloud services, enabling a seamless and secure transition to modern authentication methods, including biometrics and multi-factor authentication (MFA).
- 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 SECURITY ENGINEER 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.

- Conducted training sessions for IT staff on managing and auditing access controls, significantly reducing unauthorized access incidents by 40% within the first six months of the implementation to compliance standards.
- 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.

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.
- Managed and configured user roles and permissions in Active Directory, utilizing GPOs for enforcing security policies across the network.
- 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.
- 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.

- 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.
- Conducted comprehensive security audits using Ping Identity tools to identify and remediate potential vulnerabilities in the IAM infrastructure, aligning with best practices and compliance standards for threat detection and vulnerability management).
- 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. This initiative reduced manual security analysis time by 50% and improved threat detection speed by 40%.
- 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.
- Designed role-based, location-based, & device compliance access controls for Entra ID.

- 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 of Science in Cybersecurity,** University of Richmond 08/2024
- **Associate of Applied Science in Information Systems**, Reynolds College 05/2021

CERTIFICATIONS

- **AZ-900**, Microsoft Azure Fundamentals (In progress)
- **Cybersecurity Essentials**, Cisco 10/2021
- **IBM Cloud Essentials,** IBM 10/2021
- **Network Administration**, Reynolds College 07/202

AWARDS AND HONORS

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