NuSummit®
Cybersecurity

Customer Stories

Identity & Access Management

cybersecurity.nusummit.com

Table of content

Introduction

Elevated enterprise IAM with secure and compliant end-to-end services

Identity and access management (IAM) is essential for securing systems and data. However, the use of multiple technologies and scenarios can make it complex. Expert guidance can help streamline the IAM process, design solutions for hybrid cloud environments, and ensure compliance.

Implementing an identity and access management solution requires strategic planning, including auditing existing systems, selecting systems to integrate, and ensuring scalability, security, and automation for compliance. NuSummit Cybersecurity provides holistic IAM services from implementation to administration.

MRA remediation by upgrading CyberArk PAS solution to latest version

The client is a Fortune 50 enterprise and specialize in home loans and mortgages. The company is a prominent player in the financial industry

Current state discovery to establish a blueprint for **CyberArk v12.6 build**

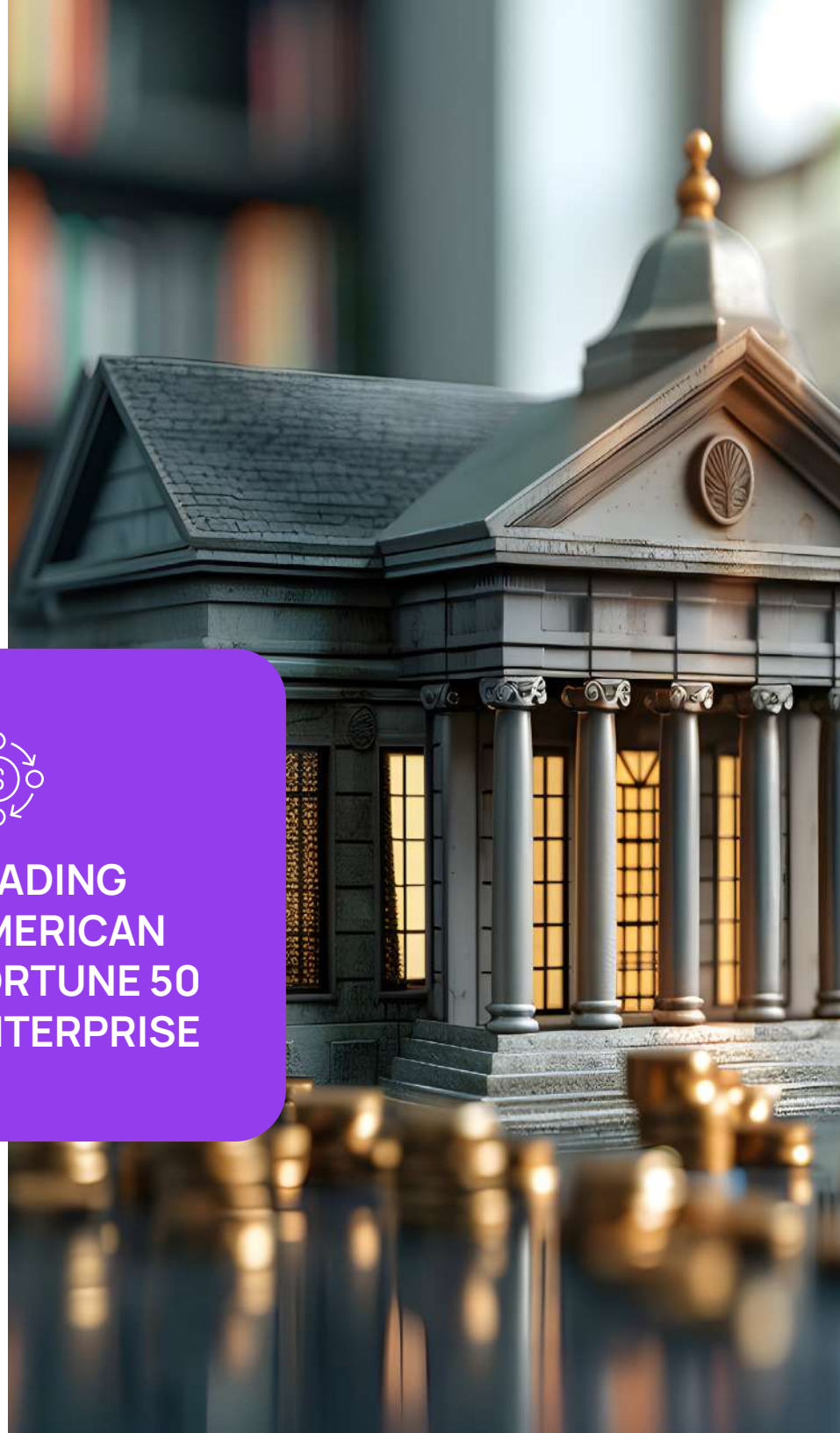
Analyze 1-year tickets for automation opportunities and implemented solutions

Upgrade CyberArk from legacy **version 12.1 to v12.6** and **migrate 100K** EPV Users and 60k Privilege Accounts

Implemented Industry **best practices and OEM** recommendation on policies and configurations

Implemented configuration management process for **version controlling of CyberArk Policies and Configuration** for Vault and Components

LEADING AMERICAN FORTUNE 50 ENTERPRISE



Challenges

- Build a team of CyberArk specialists for upgrade
- Used an agile approach with strong governance
- Communicated objectives to CXO levels
- Provided tech advisory for the new CyberArk PAS platform
- Configured solutions in non-prod and prod environments
- Conducted audits for compliance
- Closed MRAs by meeting regulatory requirements

Solution

- Build a team of CyberArk specialists
- Used an agile approach with strong governance
- Communicated objectives to CXO levels for leadership support
- Provided tech advisory for the new CyberArk PAS platform
- Implement solutions in non-prod and prod environments
- Conducted audits for compliance
- Closed MRAs by meeting regulatory requirements and provided necessary artifacts for audit closer

Outcome

- Established detailed tech blueprint for new CyberArk environment
- Created OEM and Industry best practices checklist to ensure new environment stability
- Implemented CyberArk components using scripts for ~130 servers to meet MRA deadline
- NuSummit Cybersecurity brings its partnership with CyberArk to manage the complexity of the project
- Seamless migration of 60K EPV and 100K Privileged Accounts
- Conducted full cycle of HA and DR cycles to ensure platform availability

MRA remediation by onboarding applications on SailPoint and Azure SSO

The client is one of the biggest national banks in America, headquartered in Columbus, Ohio.

15% application acceleration for meeting deadlines and MRA compliance

Kanban framework implementation with Azure dashboard for centralized tracking and executive visibility

Testing strategy enhancement reducing effort and time by **25%**

LEADING NATIONAL AMERICAN BANK

Challenges

- Integrating SailPoint IIQ with ServiceNow for mover/leaver process implementation
- Meeting regulatory requirements to close all MRA findings and observations
- Onboarding 227 applications to SailPoint IIQ and Azure SSO platform

Solution

- Formed a specialized team for SailPoint IIQ and Azure SSO implementation to onboard 227 applications in 9 months
- Conducted adoption strategy to raise awareness among app owners about SailPoint and Azure SSO benefits
- Implemented a robust governance model to track program progress and deliverables
- Developed prioritization strategy for complex app development and QA verification
- Generated compliance artifacts for MRA security observations

Outcome

- Remediated 227 applications under MRA via SailPoint IIQ and Azure SSO
- Conducted application analysis and design for onboarding to SailPoint IIQ and Azure SSO
- Recommended mover/leaver process redesign and ServiceDesk integration with SailPoint IIQ
- Achieved minimum target of onboarding 35 applications monthly to meet MRA closure deadline

Enhancing security and compliance with unified access solutions for a leading hotel chain

The client is the largest hotels and resorts chain globally, headquartered in Maryland, USA.

Foundational user journey covering registration, authentication, password recovery, and account management processes

50 million+ identities managed

Full-scale solution supporting microservices architecture using **OAuth and OpenID Connect**

LARGEST HOTELS AND RESORTS CHAIN

Challenges

- Enhancing customer engagement and revenue streams
- Ensuring secure sharing and control of consumer identity data across partner applications
- Implementing user access control across distributed microservices supporting hotel customer portals and mobile apps
- Enabling seamless user access and Single Sign-On (SSO) to applications across multiple platforms
- Managing customer data in compliance with strict privacy regulations such as GDPR and CCPA
- Preventing violations that could result in brand damage, loss of customer trust, and substantial fines
- Blocking unrestricted backdoor access to hotel services

Solution

- Conduct an accessibility assessment of registration forms and password recovery interfaces to ensure ease of navigation for users with disabilities
- Create consistent registration and password recovery interfaces optimized for various devices, including mobile phones and tablets
- Integrate analytics to monitor user interactions within the registration and password recovery forms, enabling enhancements for an improved user experience
- Implement decentralized access control solutions for microservices based on open protocols, ensuring scalability and interoperability
- Replaced the mainframe security model with a modern access

Outcome

- Enhanced security through seamless authentication for guests, ensuring an integrated access solution with a unified user experience
- Achieved compliance with local data protection laws, enabling adaptation to evolving regulations and ensuring proper management of personal data worldwide
- Unified platform integration with APIs for seamless connectivity with native and third-party applications handling customer data
- Enhanced customer analytics capabilities, providing deeper insights into each customer to monitor and improve customer experience
- Improved scalability to meet unexpected demand, enhancing customer experience and reducing the initial entry threshold through social login leverage

Enhancing security and compliance with Identity Security Cloud

The client is one of the renowned clinical research and development company in UK/US/DE

KPI-driven framework enabled the performance measurement and scoring of risk in the environment, providing transparency and visibility

Rapid Onboarding through enablers and accelerators fast-tracked the application integration with SailPoint IDN by **15%**

Advanced technological parameters enabled to **support dynamic birthright exceptions, multiple user identity types** and Bring Your Own Device (BYOD) concept

LEADING CLINICAL RESEARCH AND DEVELOPMENT ORGANIZATION

Challenges

- IAM Governance is not functional as per the required guidelines and leads to non-compliance, posing regulatory risks
- Concern with existing HRMS Integration with SailPoint IDN due to disscrepancies and data hygiene
- Onboarding of 50 legacy and clinical research applications with SailPoint IDN
- Enabling Access Certification campaign for legacy and clinical research applications

Solution

- Formed a specialized team of SailPoint IDN consultants to support the program
- Strategize to perform discovery and gap analysis and report the underlying defects that led to governance, compliance, and HRMS system discrepancies
- A specialized team laid the foundation for application onboarding by designing a rapid application onboarding strategy using enablers and accelerators
- Established KPI-driven tasks and dashboards for transparency and visibility of system risk and compliance reports to leadership
- Enabled a governance and communication model that works in a top-down approach and supports the adoption of changes

Outcome

- Achieved enhanced security posture with a robust governance system and centralized Identity Management
- Improved user experience with simplified joiner, mover, and leaver process
- Onboarded 35 applications as of date to SailPoint IDN with the help of enablers and accelerators
- Achieved compliance and enabled access certification and campaign as per industry regulations and standards, reducing risks to identities
- Overall optimization of IAM processes, resulting in increased efficiency and productivity

Enhancing IAM Security Posture and enabling to adhere Federal security requirements

American drugstore chain based in Philadelphia, Pennsylvania. It is the third-largest drugstore chain in the United States, with over 2,000 stores

CyberArk PAM roadmap for onboarding applications and service accounts through the Application Access Manager (AAM) module

Migration of legacy Web Portal Hub solution to Azure AD SSO with a record of 3 months with more than **100 Applications**

Out-of-the-box thinking to deliver SailPoint LCM while migrating from the legacy IRIS tool in a five-month timeframe deadline with internal, store, and vendor user accounts

LARGEST DRUGSTORE CHAIN

Challenges

- Managing SailPoint IIQ Life Cycle - joiner, mover, and leaver process automation
- 67 applications to be onboarded with JML process enabled to SailPoint IIQ
- Access Management Certification and campaign enablement through SailPoint IIQ
- Setup and configuration of the CyberArk PAM module and integration of privileged accounts for systems (windows and non-windows servers)
- Setting up DNA scan and process for account discovery, implementing Endpoint Privilege Management (EPM), ServiceNow integration for setting up Just-in-time access process for Vendor Access Management, and setting up PAM Governance
- Migration of the company web portal behind Azure AD for authentication and set up single sign-on (SSO) for the corporate and retail users

Solution

- Assembled SailPoint IIQ,, and Azure SSO specialisCyberArkts' teams for upgrade
- Used an agile approach with strong governance
- Strategize the delivery based on the KPI-driven model for each module
- Established SQUAD to support the project team with specialty demands
- Plan, design, and architect the solution considering FTC requirements and regulatory guidelines
- Configured solutions in non-production and production environments
- Partnership with OEM vendors for onboarding best practices to the program

Outcome

- Build a solid foundation and enabled the organization on Level 3 maturity in IAM practice
- SailPoint IIQ LCM established and onboarded the requested applications to the platform, enabling Access Management certification and ServiceNow integration
- CyberArk PAS Platform established and enhancements and functionalities like DNA scanning, integration with SIEM and ServiceNow successfully achieved along with Endpoint Privilege Management (EPM) and PAM Governance
- Onboarded the application in Azure AD SSO and configured the required application attributes for single sign-on (SSO) setup and configuration for the users from the legacy Web Portal Hub environment

CIAM Program for one of the Largest Financial Trading Platform in North America

The client is a Fortune 100 enterprise headquartered in New York. It is an American multinational investment bank and financial services company with offices in 41 countries

Extensive knowledge on **client proprietary products** and **CIAM products** to support the complex orchestration across multiple services

Re-engineered automation testing strategy, enabling rigorous testing and higher throughput reducing the testing effort and time by **~50%**

Dashboards and reports for business observations with segregated access for technical teams and leadership

LARGEST FINANCIAL TRADING ENTERPRISE

Challenges

- Modernize Customer Authentication by migrating to a Modern Authentication platform – ForgeRock
- Provide service to clients in building modern customer authentication platforms using ForgeRock Access Management, and Identity Manager
- Enhanced MFA options as a service to customers

Solution

- Comprehend the current Authentication platform, and strategize to migrate applications to a modern platform, ensuring a seamless deployment that brings significant benefits to all stakeholders
- Established a strong governance model to track, monitor, and report the program status and deliverables
- Enabled a highly skilled resource team with ForgeRock skillset and CIAM suite understanding, including legacy products
- Adopted a tailored no-impact migration strategy for legacy applications and their functionality

Outcome

- Implement and manage DevOps and quality assurance services for the newly built solutions and ensure seamless migration
- Upgrade services running on legacy technologies to modern newer platforms and integrate them with ForgeRock product to provide a modern and unified service
- Implemented ForgeRock Access Management & Identity Management, including complex microservice-based integration for various operations
- Replicated legacy functionalities into a modern platform with MFA implementation

Access Request Migration at Top 5 U.S. Hospital

U.S. based hospital chain that is one of the five biggest in the country. This chain has 2,000+ patient care sites, operates 140+ hospitals in over 20 states, and contains 300,000+ identities that need to be managed

Analyzed thousands of entitlements doctors and nurses need

Performed clean-up to remove unnecessary entitlements

Finished project ahead of schedule, so began **RBAC at no cost**

TOP 5 U.S. HOSPITAL

Challenges

- Only three months to design and deliver the solution
- Data center that housed previous access request system was being turned off
- Needed to migrate thousands of requestable roles and entitlements from the previous system to SailPoint IIQ
- The solution had to be able to create ServiceNow tickets for requests
- The solution required custom approval paths depending on the requested entitlement

Solution

- Assembled a team of SailPoint specialists
- Used an agile approach with strong governance
- Met regularly with project management team on hospital side
- Developed custom scripts to export all necessary data and import them as entitlements to SailPoint
- Customized the access request process to handle approval requirements
- Tested the solution and lead Knowledge Transfer sessions for help desk and end users

Outcome

- Migrated entire data center allowing 300,000 users to request access ahead of schedule
- Over 15,000 entitlements successfully migrated as part of effort
- Delivered project ahead of schedule allowing RBAC implementation to be started at no cost
- This was a mission critical project, as it gives Doctors and Nurses the access they need to do their life saving work

Strengthening the security posture by Implementing IAM solutions using SailPoint, Ping, RSA & CyberArk

The client is one of the biggest global fintech and payments company, headquartered in Milwaukee, Wisconsin, US

IAM Modernization: Enhanced security aligned with business objectives

Application Onboarding Success: Onboarded 600+ applications into SailPoint IIQ and Ping, exceeding targets

Efficiency Boost: Implemented CI/CD improvements and code review automation, increasing developer efficiency

Automation Implementation: Deployed Selenium for UAT and Ansible for certificate renewal, streamlining operations

LARGEST GLOBAL FINTECH COMPANY

Challenges

- Managing complex IAM solutions
- Legacy systems posed compatibility challenges, hindering automation efforts and increasing manual intervention
- Limited resources and skill gaps in IAM technologies posed challenges in project execution and support
- Operational support for IAM solutions and adherence to security compliance standards required continuous monitoring and management

Solution

- Leveraged a team of 14 IAM consultants (5 SailPoint, 5 Ping) to onboard applications efficiently in both SailPoint & Ping (Migration from CA SiteMinder)
- Implemented automation frameworks like Selenium and Ansible while conducting thorough analysis of legacy systems for compatibility
- Deployed dedicated teams of 16 IAM consultants (6 SailPoint, 9 Ping, 2 RSA) with a focus on skill development and cross-functional collaboration
- Implemented proactive monitoring mechanisms and compliance measures, supported by CyberArk PAS and RSA solutions

Outcome

- Onboarded over 600 applications in SailPoint and Ping
- Addressed compatibility issues and automated processes, reducing human efforts, and enhancing operational efficiency
- Successfully executed projects with the expertise of dedicated consultant teams, ensuring project success and customer satisfaction
- Strengthened security posture through continuous monitoring and managing privileged access, ensuring compliance with industry standards and regulations

Automated Access and Identity Management solutions for scaling workforce and application demands

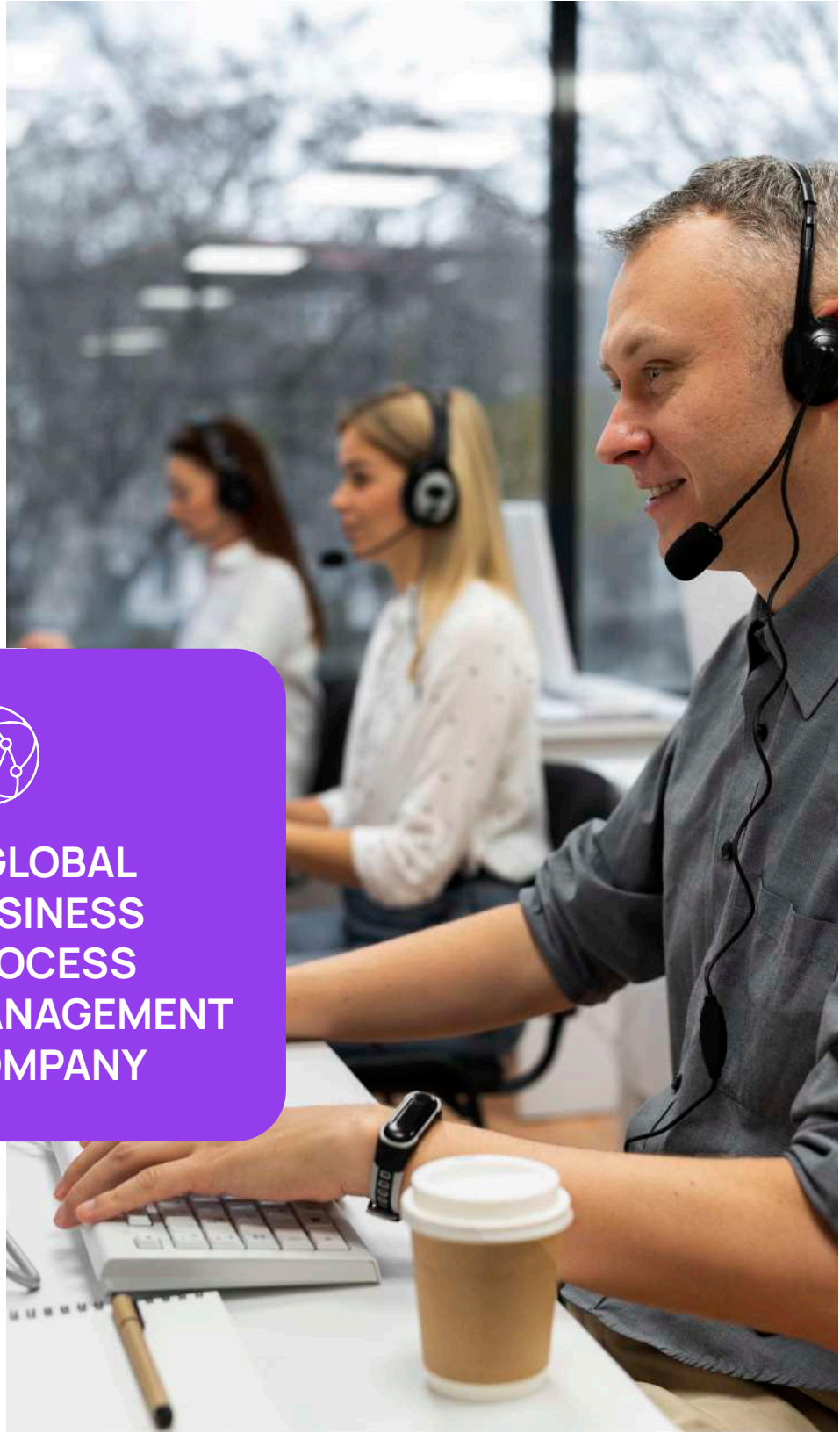
The client is a rapidly growing global business process management company with multiple business applications and 30,000 employees serving over 100 organizations

Turnaround time of 1 hour against 40 hours for access provisioning and de-provisioning

Automated Access Management for **30,000 users** and more than 5,000 project groups for **25 applications**

80% reduction in helpdesk calls

A GLOBAL BUSINESS PROCESS MANAGEMENT COMPANY



Challenges

- Human-driven processes and procedures for account provisioning and Access Management
- Lack of automated controls leading to high levels of security risk
- Increase in the number of applications due to rapid growth and rising employee strength
- Complex end-user services and handling access-related requests
- Need to sustain competitive advantage and reputation as a leading company
- Need to ensure clean audits and avoid non-compliance to maintain customer confidence and financial gains

Solution

- Automated access provisioning and removal across 25 applications, including SharePoint-based ecosystem
- Synchronization with HRMS systems to automate profile changes due to promotions or transfers across projects
- End-user empowerment for access and password management to prevent account lockouts
- Global Address List (GAL) profile management
- Approval-based account creation process
- Implementation of a time-based account expiration feature

Outcome

- Rapidly onboarded employees and temporary staff to avoid loss of productivity
- Strengthened security through timely removal of accesses
- Significantly reduced helpdesk workload by automating Identity and Access Management operations

Success stories

Leading Saudi Banking Institution

NuSummit Cybersecurity's CIAM solutions offered advanced security through features like multi-factor authentication, biometric authentication, and adaptive authentication, mitigating the risk of unauthorized access and fraud. Our CIAM platforms improved customer experience by providing seamless access to banking services across various channels and devices while offering personalized services through effective data gathering and analysis. Moreover, our services helped the bank comply with regulatory requirements such as SAMA Controls, NCA Controls, GDPR, CCPA, and PSD2 by implementing robust consent management, data encryption, and audit trails. Scalable and flexible, our CIAM platforms provided the client with a competitive advantage in delivering a seamless and secure digital experience to their customers

---

Saudi Government Authority

We facilitated the client's digital transformation and service unification objectives for citizens, expatriates, and government entities. The client reduced fraud by evaluating customer behavior and contextual factors in real-time by implementing risk-based authentication. Additionally, secure access to digital services ensured compliance with regulatory requirements while mitigating access risks across internal and cloud-based applications. The seamless user experience was enhanced by leveraging dynamic data synchronization and preventing password sharing. Federation with the national identity repository expanded access to millions of users, solidifying the client's digital infrastructure

---

Saudi Telecom Giant

Digital identity powered tech innovation and growth Enhanced security posture with robust authentication mechanisms and centralized Identity Management. Implemented multi-factor authentication (MFA) for added security

Success stories

Saudi Ministry

We enabled the Ministry to meet the Kingdom's digital transformation and service unification goals for government employees, citizens, and expatriates. By ensuring secure access to digital services and compliance with regulatory standards, we effectively mitigated access risks across both internal and cloud-based applications. We set up a federation with the national identity repository, granting access to nearly one million users, and enhancing accessibility and efficiency. Our solutions facilitated a seamless user experience through the transformation of Government E-Services using advanced technologies, including dynamic data synchronization across various platforms. We strengthened security by implementing a reliable solution to prevent password sharing and providing scalable capabilities for the rapid integration of applications with single sign-on functionality

---

Saudi Smart City

We managed external identities through a robust CIAM platform, offering end-to-end support for understanding and leveraging limitless customer opportunities. We accelerated time-to-market for business units by providing ready-to-use core CIAM functionalities, enabling quick integration of essential features and allowing the client to focus on enhancing specific offerings. With seamless sign-up processes and easy account management capabilities leveraging multiple identity providers, including social media platforms, we facilitated a streamlined user experience. Our solutions also incorporated interactive and personalized designs, reflecting the client's brand identity across all customer-facing portals. Additionally, we ensured agility and flexibility to technological trends by implementing a CIAM platform capable of keeping up with the latest advancements while maintaining scalability for future needs

About NuSummit Cybersecurity

NuSummit Cybersecurity helps build and transform cybersecurity postures to enable businesses to mitigate risks. We are a pure-play cybersecurity services company with deep expertise in Identity and Access Management, Risk Advisory, Security Verification, Managed Detection and Response, and Security Engineering services. Our unique products and services help businesses build and transform security postures while mitigating risks. Our focus is to strengthen security resilience by minimizing the occurrence of attacks, threats, and risks so that you can drive change, innovate, and accelerate growth.

For more information,
visit us at **cybersecurity.nusummit.com** or
write to us at **cybersales@nusummit.com**

Cupertino | Dallas | Jersey City | Ottawa | Riyadh | Dubai
Mumbai | New Delhi | Bangalore