NAVIGATING SAILPOINT INTEGRATION: TIPS FOR SMOOTH IMPLEMENTATION AND DEPLOYMENT

ONEIDENTITY: FIVE PRIVILEGED ACCESS MANAGEMENT BEST PRACTICES TO THRIVE IN THE HYBRID AND MULTI-CLOUD ERA

THALES: CIAM: FOSTERING COMPLIANCE, BUILDING TRUST

UNLOCKING IDENTITY SECURITY: HOW IDENTITY BRIDGE IS REVOLUTIONIZING IAM

Securology

An IT Security Magazine by Avancer Corp.

VOLUME 2: EDITION 1

Welcome to Securology – Your Gateway to Identity Security Insights

Stay ahead in the fast-evolving world of Identity and Access Management (IAM) with Securology. From expert analyses on cutting-edge technologies like AI and RBAC to actionable strategies for tackling today's identity security challenges, every edition is packed with insights to help you secure your digital future.

Why Read Securology?

- Discover the latest advancements in IAM.
- Gain thought leadership from top experts in the field.
- Explore real-world applications and success stories across industries.

Be a Part of the Conversation

Visit us at www.securology.us to explore the latest issue, learn more, or submit your articles today.

Let's shape the future of identity security together!

avancer
Simplified IT Security

Transform Your Identity Security with Avancer’s Expert IAM Consulting

Strengthen digital security with Avancer Consulting’s IAM solutions for secure access, streamlined operations, and compliance.

Modernization and security

Upgrade legacy systems for enhanced security and performance.

Partner with Avancer to secure, simplify, and strengthen your identity management strategy. Ready to future-proof your access control?

Implementation Services

Seamlessly deploy IAM solutions tailored to your business needs.

IAM Managed Services

24/7 expert management for reliable, secure access control.

Assessment Services

Identify and address IAM gaps with in-depth analysis.

Talk to Our IAM Experts »

FROM THE EDITOR

Welcome to this edition of Securology, dedicated to the transformative role of Artificial Intelligence (AI) in identity security. In today's rapidly changing threat landscape, AI has become pivotal, from driving precision in Vulnerability Assessment and Penetration Testing (VAPT) to optimizing Role-Based Access Control (RBAC) with predictive analytics and dynamic role management. Our cover story delves into how AI-driven RBAC is reshaping identity governance, providing deeper security and operational efficiency.

We're also excited to feature insights from our partners at Thales and OneIdentity, whose articles bring valuable perspectives on Customer Identity and Access Management (CIAM) and Privileged Access Management (PAM), respectively. A special thanks goes to Girish Koppar for his impactful article on protecting patient data in the digital age, a priority for today's healthcare providers.

As always, our goal with Securology is to empower organizations with actionable strategies that go beyond compliance, building resilient, future-ready security frameworks. We hope this issue equips you with the knowledge to stay secure and thrive in a complex digital world. Enjoy, and we look forward to your feedback!

Asha Dey

EDITOR-IN-CHIEF

OUR TEAM

ARUN MEHTA
President

ASHA DEY
Editor-in-Chief

ROOPA GUPTA
Head of Strategic Alliance

RAJESH MITTAL
CTO

Email Id: info@securology.us
Phone: +1 (609) 632-1285
Website: securology.us
Editorial Contact:
editorial@securology.us
Advertising Contact:
advertising@securology.us
Securology
Print - ISSN 2576-3369
Online - ISSN 2576-3377
is published by Avancer Corporation, 30 N Main Street, Ste 201, Cranbury, NJ 08512
Image Source: Canva Premium

Disclaimer: The publisher makes every effort to ensure the correctness of the content. However, we accept no responsibility for any error or omissions. Unsolicited material, including photographs and manuscript, is submitted entirely at owners risk and the publisher accepts no responsibility for its loss, damage or return. The views expressed in each article is opinion of the author and does not necessarily reflect opinion of Securology or Avancer Corporation. All rights reserved. Avancer Corporation holds exclusive copyright of all the materials published in the magazine, in all formats, unless otherwise mentioned. Reproduction of material in whole or in parts in any format—print or digital—without permission is prohibited in English or any other language. All disputes are subject to exclusive jurisdiction of competent courts and forums in New Jersey. All advertisements and advertorials are the responsibility of the advertisers, Avancer Corporation does not assume any liability for services or products advertised herein.

TECH DESK

With today's digital environments becoming more complex, the need for advanced identity and access solutions is critical. At Avancer, we are dedicated to designing IAM frameworks that not only secure but also simplify access across multi-environment architectures. This issue showcases several key innovations in our IAM portfolio that I'm pleased to share.

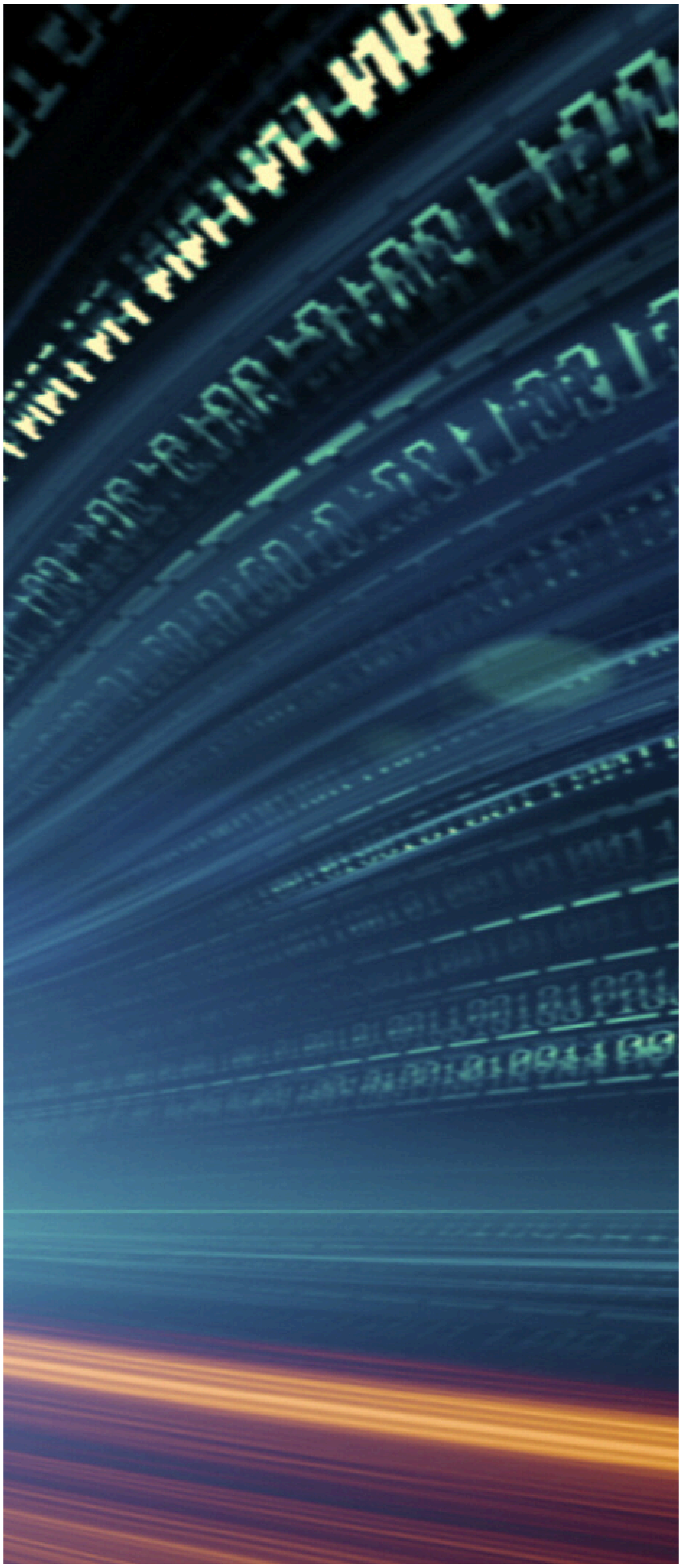
Leading these advancements is our Identity Bridge platform. Built with an API-first approach, Identity Bridge enables seamless integration across cloud, on-prem, and hybrid setups. It allows organizations to consolidate identity processes, automate compliance, and precisely control access—all essential for enhancing both security and operational efficiency.

We also explore our Factory Model, a scalable methodology we've refined to streamline application onboarding across diverse ecosystems. Finally, we delve into AI-driven Role-Based Access Control (RBAC), where predictive analytics transform traditional role management into a proactive system that adapts to evolving organizational needs. This offers unprecedented control and compliance in highly regulated industries.

I hope these insights inspire you to harness AI and scalable architecture to advance IAM in your organization.

Rajesh Mittal
RAJESH MITTAL
CTO, AVANCER CORP.

TABLE OF CONTENTS



IN FOCUS

FEATURE

COVER STORY

Securology

GUEST POSTS

CASE STUDIES

UNLOCKING IDENTITY SECURITY: HOW IDENTITY BRIDGE IS REVOLUTIONIZING IAM

Managing identities and securing access across multiple applications has become increasingly complex. If you're expanding your business across digital ecosystems, you know the challenges of balancing security, efficiency, and cost. Here's where Identity Bridge steps in—a game-changer in the Identity and Access Management (IAM) world.

Identity Bridge, an API-based IAM platform, simplifies identity management, enhances security, and maximizes ROI. With its ability to streamline processes like provisioning, managing dormant accounts, and ensuring compliance, Identity Bridge reshapes IAM with a focus on customization and cost-effectiveness. Let's explore how it can transform your identity management.

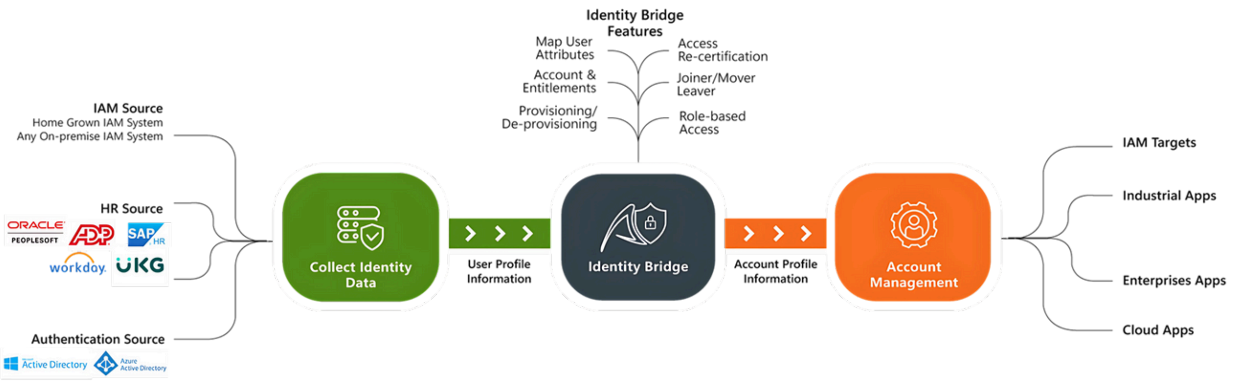
How Does Identity Bridge Work?

At the heart of Identity Bridge is its API-first architecture, designed to seamlessly integrate identity management into your existing digital infrastructure. This API-based approach enables businesses to manage user identities, enforce access policies, and secure their environments efficiently, regardless of where their applications reside—on-premises, in the cloud, or in hybrid environments.

The flexibility provided by Identity Bridge's APIs allows organizations to customize their IAM solutions based on their unique needs, whether integrating legacy systems or rapidly scaling to meet business growth. This approach simplifies identity management by ensuring all systems, from HR databases to third-party applications, communicate smoothly, providing a centralized and secure method for managing access across the organization.

The API-driven framework of Identity Bridge collects data from multiple sources, including homegrown IAM systems, HR databases, and authentication sources like Active Directory. This collected user profile information is utilized by Identity Bridge to perform various functions related to identity and access management, such as mapping user attributes, creating accounts and

Identity Bridge Process Flow



entitlements, provisioning and deprovisioning, performing access recertification, and undertaking role-based access grants.

Identity Bridge serves as a crucial component in managing the end-to-end identity lifecycle, ensuring that users have appropriate access to resources based on their roles and responsibilities. Additionally, it facilitates secure authentication to various applications and services. This integrated approach is essential for organizations to maintain efficient and secure access control across their diverse IT landscape.

Transforming Identity Management with Identity Bridge

Identity Bridge offers a myriad of use cases that cater to the diverse needs of modern businesses. Here are some of the key areas where our solution can make a significant impact.

Streamlined Provisioning and Deprovisioning: Drive Efficiency and Maximize ROI

Ever found yourself bogged down by manual tasks like granting or revoking access to employees? It's not only time-consuming but risky too. Identity Bridge automates these processes, so when a new employee joins or leaves, access is granted or revoked instantly—no delays, no gaps.

What does this mean for you? Fewer security risks and faster onboarding. The platform takes care of the heavy lifting, ensuring the right people have the right access at the right time, without the constant need for human intervention.

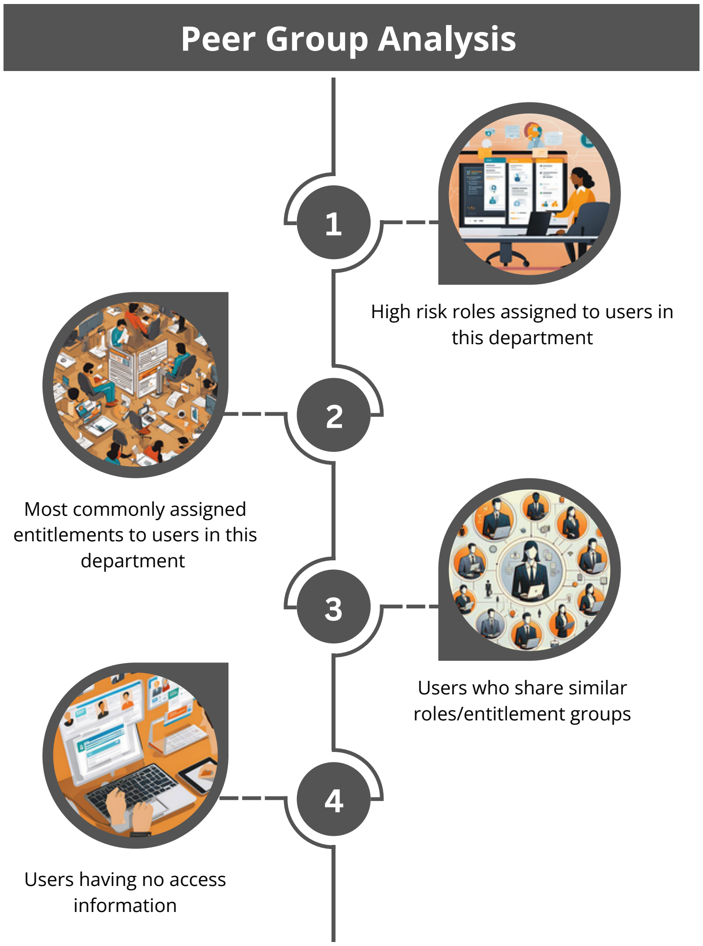
And here's where we really stand out—Identity Bridge is built to be highly customizable. We understand that no two businesses are alike, so our solution is tailored to your specific needs, allowing you to create workflows that best suit your organization. The result? Greater efficiency at a fraction of the cost of traditional IAM systems.

Orphan and Dormant Accounts: Eliminate Security Risks

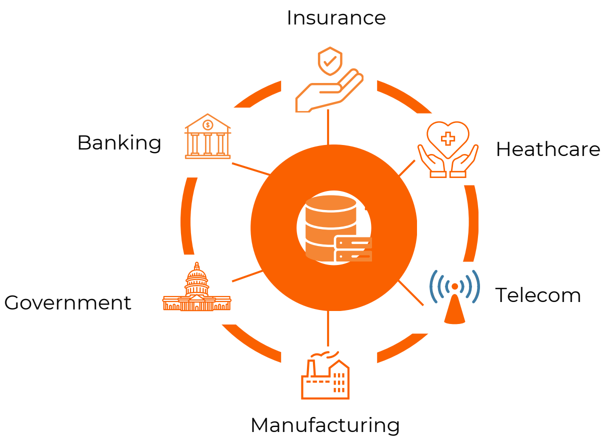
As we are all aware that unused accounts, also called orphan accounts, are one of the biggest security risks. These accounts can sit idle for months, sometimes even years, and they're prime targets for cybercriminals.

But with Identity Bridge, this won't be a concern anymore. Our solution actively monitors and flags orphan and dormant accounts, ensuring they're deactivated before they become security vulnerabilities. For you, this means peace of mind—knowing that every access point is secure and every risk is mitigated.

We keep things simple and cost-effective by automating these processes. By reducing manual oversight, your IT team is freed up to focus on more critical tasks while security remains tight.


Peer Group Analysis
1
High risk roles assigned to users in this department
2
Most commonly assigned entitlements to users in this department
3
Users who share similar roles/entitlement groups
4
Users having no access information

Tailored Identity Solutions Across Sectors



Identity Bridge is industry-agnostic, offering adaptability and configurability to help organizations tailor workflows and settings to address their unique identity management challenges.

Stay Compliant, Stay Secure: Meeting Essential Standards

In the current regulatory landscape, compliance is non-negotiable. For industries such as finance or healthcare, the stakes are even greater, with stricter standards and heightened risks. Identity Bridge simplifies the complexity by automating compliance processes, ensuring that your organization adheres to industry-specific regulations without adding to your workload.

Here's the best part: our solution is designed to be scalable and affordable. You don't need to invest in costly infrastructure upgrades. Identity Bridge integrates seamlessly into your existing systems, whether they're on-prem, in the cloud, or hybrid. The flexibility to customize access controls and workflows means that as your business grows, your IAM solution grows with you—without skyrocketing costs.

> **We provide a centralized, customizable platform that eliminates manual errors and ensures that new applications are integrated securely and quickly. The intuitive workflows guide your team through every step, saving time and reducing complexities.**

Audits and Reports: Compliance Made Easy

If you've ever had to prepare for an audit, you know how tedious and stressful it can be. What if your IAM system could automatically provide you with real-time reports and audit trails? That's exactly what Identity Bridge does.

Our solution ensures that you always have a comprehensive view of who has access to what—and when. Whether for internal audits or meeting external regulatory requirements, Identity Bridge streamlines the reporting process, ensuring effortless compliance every step of the way.

With customizable reporting features, you can tailor audit reports to fit your organization's exact requirements, whether you're adhering to HIPAA, GDPR, DPDP Act or any other regulation. This isn't just about ticking boxes; it's about making compliance stress-free and cost-effective.

Onboarding New/Industry-Specific Applications: Seamless and Flexible

Bringing new or industry-specific applications into your IT environment can be daunting. The manual processes involved in onboarding them often lead to delays, and inconsistencies in access control can leave your organization vulnerable. Identity Bridge changes the game by making app onboarding simple.

We provide a centralized, customizable platform that eliminates manual errors and ensures that new applications are integrated securely and quickly. The intuitive workflows guide your team through every step, saving time and reducing complexities.

No more juggling multiple systems or struggling with inconsistent access policies. Whether your business is scaling or integrating new apps for growth, Identity Bridge ensures the process is smooth, secure, and cost-efficient.

Role-Based Access Management: Precision Control for Your Organization

Identity Bridge offers robust Role-Based Access Management (RBAC) capabilities designed to simplify identity governance. With our innovative “In Clause” feature, administrators can efficiently manage access rights by specifying inclusive criteria for role assignments. This ensures precise control over user privileges, allowing you to manage who has access to what in a clear and structured manner.

Additionally, Identity Bridge extends its support to multiple target applications, seamlessly orchestrating entitlements across diverse systems. Our platform enhances the user experience by providing a streamlined, intuitive interface for role administration. This comprehensive role management functionality not only simplifies identity governance but also strengthens security and compliance across your organization's ecosystem.

Key Benefits:

1

API-DRIVEN CUSTOMIZATION:

Tailor IAM processes to suit your specific business needs using flexible APIs.

2

COST EFFICIENCY:

Reduce operational costs with automation and streamlined processes.

3

COMPLIANCE MADE EASY:

Automate audit trails and regulatory reports.

4

SCALABILITY:

Grow your IAM capabilities as your business expands.

Secure Data Access and Encryption: Protecting What Matters Most

When it comes to protecting sensitive information, Identity Bridge implements robust security protocols, including authentication mechanisms, access controls, and advanced encryption techniques. Our strong authentication and authorization protocols safeguard data from unauthorized access, reducing the risk of data breaches and ensuring data integrity.

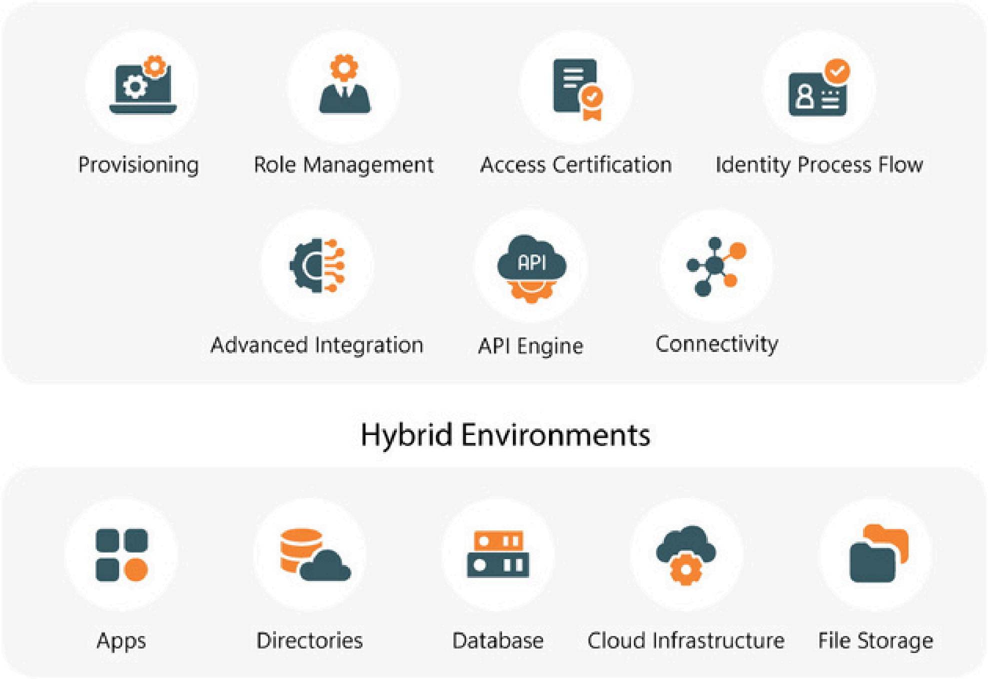
Our password encryption feature keeps sensitive login credentials shielded from potential threats. Additionally, our Key Management capability enables organizations to encrypt user fields, ensuring the confidentiality of critical information. Identity Bridge goes a step further by allowing organizations to bring their own encryption keys, providing an additional layer of control and security.

Why Identity Bridge? Your Path to Cost-Effective, Customizable IAM

At its core, Identity Bridge is designed to deliver value by being both cost-effective and highly customizable. Whether it’s automating tedious tasks, securing dormant accounts, or easing compliance reporting, every feature is tailored to meet your unique needs.

We understand the budget pressures many businesses face, which is why we built Identity Bridge to be affordable, without sacrificing functionality. Our flexible pricing model and scalable architecture mean that you get all the benefits of a top-tier IAM solution at a fraction of the cost.

Identity Bridge Marketecture



Identity Bridge Marketecture is built on a foundation of scalability, designed to grow with your business. Our architecture adapts to your unique needs, ensuring that identity management scales effortlessly. Identity Bridge thrives in hybrid ecosystems.

Security and efficiency are non-negotiable for businesses, and with Identity Bridge, you don't have to choose between them. Our API-based solution enhances security, cuts operational costs, and optimizes processes seamlessly. Leveraging advanced technology and industry best practices, Identity Bridge helps your organization achieve compliance and excel in today's competitive landscape. Trust Identity Bridge to be your partner in navigating the complexities of identity management, allowing you to focus on what matters most—growing your business.

Ready to revolutionize your IAM strategy? Identity Bridge offers a flexible, scalable, and cost-effective solution that evolves with your business. Let us help you unlock the true potential of identity security.

Contact us for a demo and discover how we can tailor the perfect IAM solution for you.

We designed Identity Bridge to deliver powerful IAM capabilities with seamless integration and scalability, ensuring robust security without complexity. Furthermore, our flexible pricing model allows businesses to access top-tier features at competitive cost.

IDENTITY BRIDGE

EFFICIENT. SEAMLESS. ROBUST.

Identity Bridge: Power of Seamless Identity and Access Management

Manage identities, automate onboarding/offboarding, and secure application access effortlessly with Identity Bridge, a cutting-edge API-based platform.

- Real-time user provisioning
- Enhanced security & encryption
- Easy application integration
- Compliance automation

Schedule a Demo ›

SCALING UP: BEST PRACTICES FOR SEAMLESS INTEGRATION OF LARGE APPS USING THE FACTORY MODEL

- ARUN MEHTA

Feature

As businesses expand, they often find themselves dealing with an overwhelming number of applications—some cloud-based, others on-premise—each requiring unique management and access controls. What once started as a streamlined digital ecosystem can quickly turn into a sprawling maze of applications, making it increasingly difficult to track and manage user access effectively. This complexity can slow down operations, increase security risks, and create bottlenecks in the integration process. Ensuring that the right users have the appropriate access to each application becomes a daunting challenge, one that demands a more strategic approach. One such challenge was faced by a prominent US-based insurance company that approached us at Avancer. Their digital infrastructure had expanded dramatically, ballooning to over hundreds of applications that ranged from customer management platforms to internal data systems.

These applications operated in silos, each with its own security model and governance structure, which not only created integration headaches but also made their IAM system difficult to manage. The reliance on manual processes exacerbated the situation, leading to inefficiencies and a heightened risk of security breaches. Adding to the complexity, the company's existing IAM system was significantly underutilized.

Without streamlining and automation, their IAM practices were unable to effectively review, monitor, or manage user access across their various applications.

Compliance became increasingly difficult as the team struggled to maintain visibility over user access, while integrating applications from different technology stacks proved cumbersome and time-consuming. This growing complexity and the lack of a unified, automated approach made their digital ecosystem both inefficient and vulnerable.

The Turning Point: Enter the Factory Model

At Avancer, we understood that adopting the factory model—much like an assembly line—promised to automate and standardize repetitive integration tasks. However, simply implementing the model wasn't enough; applying best practices was crucial to its success.

Here's how we at Avancer helped the company achieve seamless integration.

As the company's challenges continued to grow, it became evident that a more structured and scalable solution was required to handle their expanding ecosystem of applications. This is where Avancer's Factory Model came into play. Inspired by the efficiency of an assembly line, the Factory Model is designed to automate and standardize the repetitive tasks involved in integrating multiple applications. By creating a repeatable and structured process, it streamlines onboarding, reduces errors, and ensures consistency across the board.

However, adopting the Factory Model wasn't just about automation—it was about leveraging best practices to ensure long-term success and scalability.

Yet, implementing the Factory Model alone wasn't sufficient. We customized it to align with the company's unique requirements, integrating industry best practices at every step. From evaluating their application landscape to automating critical workflows, the tailored model provided a robust framework for seamless and scalable integration.

> **Ensuring that the right users have the appropriate access to each application becomes a daunting challenge, one that demands a more strategic approach.**

Here’s how we at Avancer helped the company achieve seamless integration.

Best Practices in Action

1 Assessing and Mapping the Application Ecosystem

CHALLENGE:

Our initial challenge was gaining a clear understanding of the organization's vast app ecosystem. With hundreds of siloed applications spread across various departments, the integration landscape was fraught with complexity and potential pitfalls. Without a thorough assessment, any integration would be inefficient and prone to errors.

OUR APPROACH:

We began by conducting a comprehensive audit of the applications, identifying overlaps, dependencies, and the most critical integration points. This detailed mapping allowed the company to gain deep visibility into their digital infrastructure. It also provided us with the foundation to create a phased integration roadmap, ensuring an efficient, agile, and structured process tailored to the company's needs.

Our Integration Roadmap Process:

1. Creating an integration plan for designing, building and testing the integration process in an effective and predictable way.
2. Defining metrics and standardized processes to help integrate applications across all the domains in an enterprise.
3. Deploying process that is proven over time for being highly reliable and cost-effective.
4. Providing support to the internal client team with various skill sets and resources.

Best Practice: Start with a detailed assessment of the application landscape to identify key integration needs and challenges. Map dependencies, prioritize critical applications, and create a roadmap for phased implementation.

2

Standardizing Processes for Consistency

CHALLENGE:

The existing integration processes were inconsistent across teams, leading to errors, rework, and wasted time. Without uniformity in the approach, the lack of standardization caused delays and inefficiencies.

OUR APPROACH:

We implemented standardized processes across the board, ensuring that every integration followed the same protocols. We created reusable components and templates that made each integration smoother, regardless of the application or department. To further streamline and align the process, we introduced the T-shirt sizing model, assessing them based on complexity and integration requirements.

Division of apps in T-shirt size model

At Avancer, we also assess the applications as per its size. Such a concept of application sizing is based on data source footprint, business unit usage, internal and external applications, and varying degree of complexity. We categorize the apps using the metaphor of t-shirt sizes. Additionally, feel free to define your own set of parameters to simplify the process of integrating the number of apps you may want to bring to your IAM platoform.

Size	Description
XL	This application set includes four or more combinations of entitlement stores, such as application, database, server, and privileged access. For example, it may consist of an application entitlement store, a database entitlement store, a server entitlement store, and a privileged entitlement store, all integrated for comprehensive application reviews.
L	This application set includes any three combinations of entitlement stores, such as application, database, server, or privileged access. For example, it may comprise an application entitlement store, a database entitlement store, and a server entitlement store, enabling a comprehensive application review.
M	This application set includes any two combinations of entitlement stores, such as application, database, server, or privileged access. For example, it may consist of an application entitlement store and a database entitlement store, supporting an in-depth application review.
S (Internal)	This application set includes a single entitlement source, such as an application, database, or server. For example, it may consist of only an application entitlement store or an application entitlement store combined with groups from Active Directory (AD).
XS	This application set relies solely on Active Directory (AD) entitlement store.
S (External)	External applications that need to be integrated with IAM platform.

Best Practice: Standardize integration processes by creating repeatable templates and components. This improves consistency, reduces errors, and accelerates the integration process. Use models like the T-shirt sizing method to categorize applications and streamline integration efforts, improving consistency, reducing errors, and accelerating the integration process.

3 Automation for Speed and Efficiency

CHALLENGE:

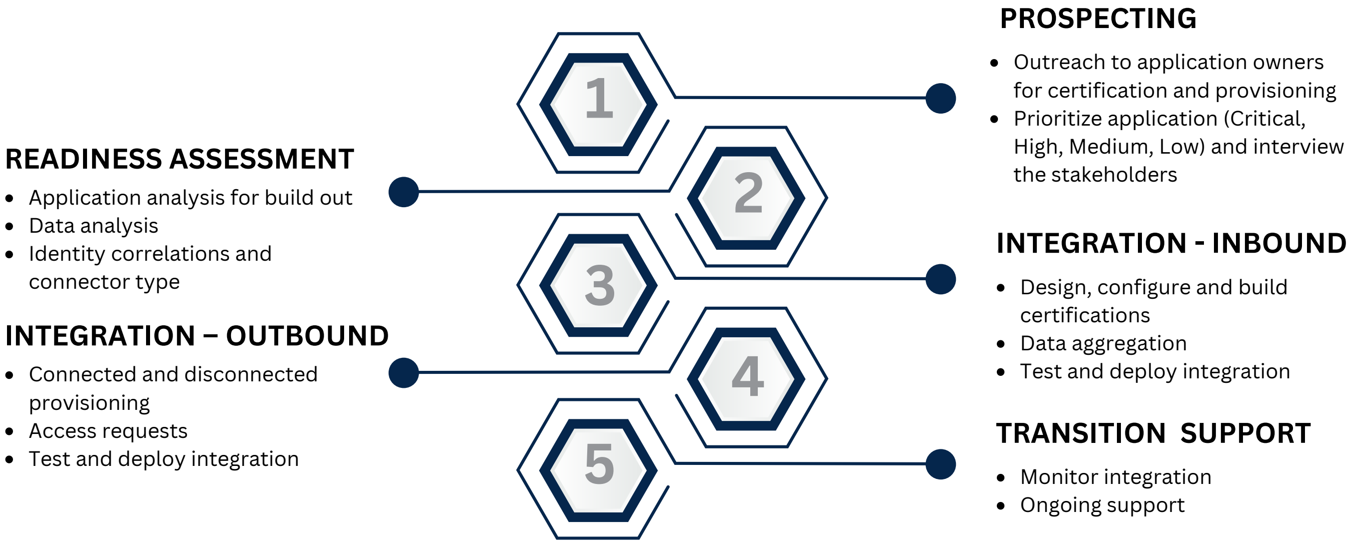
Manual processes were not only slow but also prone to human error. The IT team found it difficult to keep up with the increasing number of applications, leading to inefficiencies and bottlenecks.

OUR APPROACH:

To address the inefficiencies of manual processes, we introduced automation through our Five-Pronged Factory Model—a system specifically designed to streamline and accelerate critical tasks like data synchronization, workflow management, and user provisioning.

This approach empowers organizations to move from reactive, manual methods to proactive, automated operations. By simplifying repetitive tasks and reducing the risk of human error, our model ensures faster, more efficient integrations that keep pace with growing business demands.

What sets Avancer apart is the unique adaptability of our Factory Model. While it provides a standardized, assembly line structure to ensure consistency and scalability, we customize it to fit each client's specific needs. Every step in the process is meticulously designed to keep teams aligned, minimize errors, and accelerate deployment. This blend of structured reliability and tailored solutions enables us to tackle even the most complex integration challenges with precision and speed, delivering unmatched results that elevate business performance and security.



PROSPECTING

- Outreach to application owners for certification and provisioning
- Prioritize application (Critical, High, Medium, Low) and interview the stakeholders

READINESS ASSESSMENT

- Application analysis for build out
- Data analysis
- Identity correlations and connector type

INTEGRATION - INBOUND

- Design, configure and build certifications
- Data aggregation
- Test and deploy integration

INTEGRATION – OUTBOUND

- Connected and disconnected provisioning
- Access requests
- Test and deploy integration

TRANSITION SUPPORT

- Monitor integration
- Ongoing support

Best Practice: Automating repetitive tasks such as data synchronization, workflow management, and user provisioning not only improves speed and efficiency but also minimizes the risk of human error. Leveraging our Five-Pronged Factory Model ensures scalability and consistent integration processes across an expanding application landscape. This allows internal teams to focus on more strategic, high-value initiatives.

4 Comprehensive Application Integration

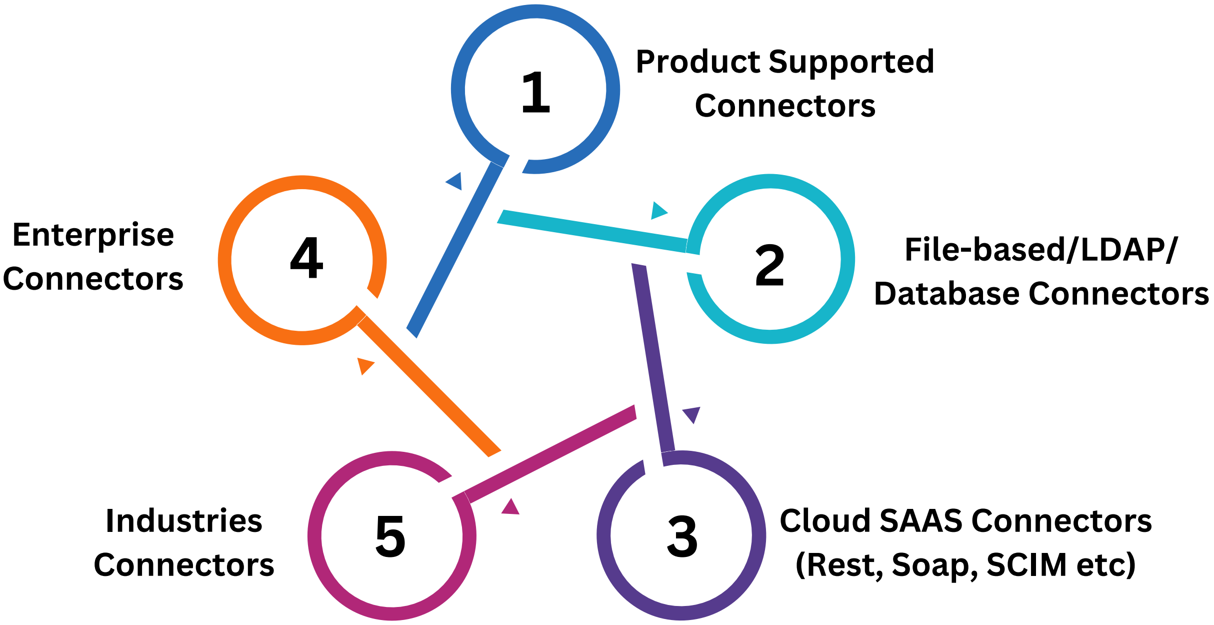
CHALLENGE:

The complexity of integrating multiple applications posed significant challenges for the organization. With a wide array of applications—each with unique integration requirements—there was a risk of overlooking critical integration points, which could hinder the effectiveness of the IAM solution.

OUR APPROACH:

To address this challenge, we conducted a thorough review of all integration points across the organization's digital ecosystem. This included leveraging product-supported connectors, such as Database Connectors, Webservice Connectors, Enterprise Connectors, and Industry-Specific Connectors. Our team ensured that each type of connector was correctly implemented and configured to work with the IAM system. We standardized the integration protocols for each application, verifying that every connection point was optimized for functionality, security, and performance.

Integration Points


1
Product Supported Connectors
2
File-based/LDAP/ Database Connectors
3
Cloud SAAS Connectors (Rest, Soap, SCIM etc)
5
Industries Connectors
4
Enterprise Connectors

Best Practice: Ensure that all integration points are accounted for by conducting a comprehensive review of the application ecosystem. Utilize a range of product-supported connectors, ensuring compatibility and efficiency across database, web service, enterprise, and industry-specific connectors. Standardizing the integration process and customizing connectors for specific application needs ensures seamless, secure, and scalable integration into the IAM environment.

5 Cross-Team Collaboration and Communication

CHALLENGE:

Integration challenges extended beyond technical issues—ineffective communication between departments often resulted in delays, misaligned priorities, and confusion.

OUR APPROACH:

We fostered cross-team collaboration by setting up clear communication channels and alignment meetings between various departments. This ensured that everyone was on the same page regarding timelines, expectations, and responsibilities. Our goal was to create a unified approach where every team could contribute to the success of the integration process.

To achieve this, we implemented:

- Weekly project status report detailing the progress, plan, updates, risk/issues mitigation
- Phased demos/walkthroughs of identity and access functionality, based on project milestones
- Bi-weekly IAM steering committee meeting to govern and guide the project
- On-demand peer-to-peer project update meeting to address any issues

Best Practice: Encourage cross-team collaboration with clear communication channels. Regular updates and alignment meetings ensure that all teams are working together toward common integration goals.

6 Training and Adoption

CHALLENGE:

Successful implementation of any new system requires not just technical integration but also user buy-in and engagement. Without proper training and support, employees may struggle to adapt to new processes, leading to underutilization and frustration.

Best Practice: Invest in thorough training and change management initiatives to promote user adoption of new systems. Engage stakeholders early in the process and provide continuous support to ensure everyone is equipped to maximize the benefits of the integrated solution. This commitment to training creates a more competent workforce, drives utilization, and solidifies the success of the integration efforts.

OUR APPROACH:

We emphasized the importance of comprehensive training and ongoing support to ensure the smooth adoption of our Factory Model. We developed tailored training programs that educated users on the system's features, benefits, and workflows, including hands-on workshops, detailed documentation, and continuous feedback sessions to address concerns.

Additionally, we implemented change management strategies that fostered a culture of collaboration and openness. By actively involving key stakeholders in the integration process, we ensured their insights were considered, further enhancing user engagement. This focus on training and support empowered teams to fully utilize the new system and facilitated a smoother transition, ultimately leading to greater operational efficiency and satisfaction.

In Conclusion:

By leveraging the Factory Model and our expertise at Avancer, the company successfully onboarded hundreds of applications into their IAM environment. This strategic approach delivered several key benefits: streamlined integration through standardized processes and automation, enhanced compliance with automated certification processes and improved audit performance, increased agility enabling faster onboarding and scalability, and improved visibility with comprehensive access reviews and reporting. As a result, the company now operates with a robust, secure, and compliant IAM system, significantly enhancing their business performance and establishing a scalable framework poised to support future growth.

Our Factory Model Helps:

1. To scale-up process of on-boarding large number of apps across functions and domains
2. To initiate digital transformation in a faster and efficient manner
3. To reduce implementation cost
4. To onboard apps in a reliable manner
5. To improve access to data in a secure manner

TOP IAM TRENDS TO WATCH OUT FOR

As digital transformation accelerates, Identity and Access Management (IAM) continues to evolve, adapting to emerging security threats and business demands. Here are the key trends driving the future of IAM.

01. Password-less Authentication

Reducing password dependency with biometrics, OTPs, and device-based logins for improved security and user experience.

02. Zero-Trust Architecture

Adopting a "never trust, always verify" approach to secure every access point.

03. AI-Driven IAM Systems

Leveraging AI for real-time risk analysis, automated threat detection, and predictive security insights.

04. Decentralized Identity

Shifting control of identity data to users, enhancing privacy and data security.

05. IGA Automation

Leveraging IGA automation with identity management products as fulfillment engines for streamlined provisioning and governance.

06. Convergence of IAM and PAM

Combining IAM with Privileged Access Management (PAM) for holistic access control across all user levels.

07. ITSM Driven Access Approvals

Integration of ITSM-driven access approvals into IAM workflows for enhanced efficiency and compliance.

NAVIGATING SAILPOINT INTEGRATION: TIPS FOR SMOOTH IMPLEMENTATION AND DEPLOYMENT

- SANJEEV MENDHIRATA

Feature

At Avancer, we have partnered with organizations across various industries to secure their digital identities and protect their systems through the effective deployment of IAM solutions, including SailPoint's IdentityIQ and Identity Security Cloud (ISC). Our journey with SailPoint integrations has evolved significantly, revealing that a successful integration isn't just about the technology—it's about understanding each organization's unique needs and tailoring the implementation to deliver long-term success. By customizing implementations to align with specific business goals, we ensure that our clients achieve not only immediate results but also long-term security and operational success.

While every project is different, there are key strategies we've developed that consistently lead to smooth, efficient deployments. Through numerous implementations, we've refined our processes and created best practices to guide us through every SailPoint deployment. These practices ensure that IAM integrations are aligned with business goals, provide scalability, and support regulatory requirements without overwhelming the organization.

Here’s how we’ve approached SailPoint integrations, and the steps we’ve taken to ensure successful outcomes.

Effective Governance: Building a Solid Foundation

We believe that every successful IAM project begins with strong governance. Whether it's assigning ownership to IT security teams, compliance officers, or business leaders, we've found that having these roles in place early on ensures smoother collaboration down the line. A well-structured governance model not only strengthens security but also establishes a culture of compliance and transparency across the organization. By defining clear roles and responsibilities, it mitigates risks associated with access control violations and minimizes human error.

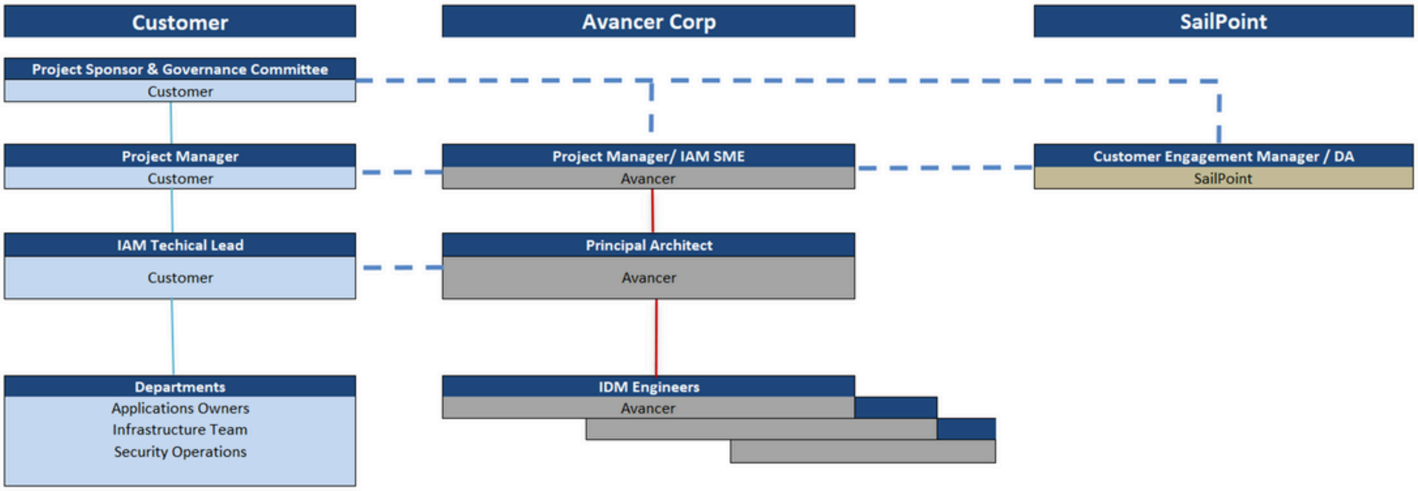
Furthermore, we customize governance frameworks to suit each organization’s specific needs, ensuring seamless integration with their existing processes. This proactive approach enables companies to anticipate potential challenges, adjust quickly to regulatory changes, and maintain compliance across evolving business landscapes. Ultimately, effective governance fosters long-term resilience and agility in identity management practices.

Streamlining Collaboration: Bringing Stakeholders Together

Collaboration has always been key to any IAM project’s success, and this holds especially true for SailPoint implementations. We’ve built a Governance Model that ensures seamless communication between clients, Avancer, and SailPoint, throughout the project lifecycle.

By ensuring open channels of communication, we prevent silos and encourage real-time updates, keeping everyone aligned with the project’s objectives. This clarity not only enhances transparency but also enables us to stay agile, adapting to changes quickly and efficiently.

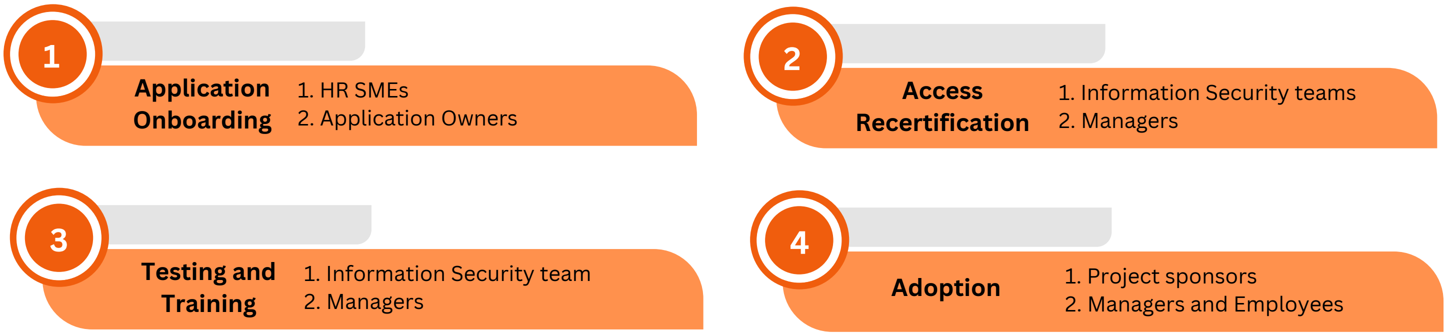
> **Furthermore, we customize governance frameworks to suit each organization’s specific needs, ensuring seamless integration with their existing processes**



Our Team Engagement Model takes this collaboration a step further by coordinating key stakeholders across crucial phases like onboarding, recertification, and testing. This structure brings teams together early, ensuring that everyone from HR, security, IT, and management has a seat at the table.

By leveraging this unified approach, we streamline decision-making processes, increase stakeholder engagement, and optimize resource allocation. Ultimately, this leads to better project outcomes, as teams work cohesively toward proactive risk management and timely delivery, keeping the IAM solution aligned with both business goals and security needs.

Team Engagement Model



1 **Application Onboarding**
1. HR SMEs
2. Application Owners

2 **Access Recertification**
1. Information Security teams
2. Managers

3 **Testing and Training**
1. Information Security team
2. Managers

4 **Adoption**
1. Project sponsors
2. Managers and Employees

Structured Application Onboarding: Setting the Stage for Success

Application onboarding is one of the most critical aspects of any IAM implementation. A well-structured onboarding approach not only simplifies the integration process but also ensures that each application is onboarded with the appropriate access policies in place. This method reduces risk, enhances security, and leads to a more cohesive IAM environment that supports organizational goals.

We've adopted a three-pronged approach to simplify the onboarding process and minimize security risks:

APPLICATION ONBOARDING PROCESS:

Breaking down the onboarding into clear, actionable steps ensures smooth execution. We categorize applications, assess their importance, and allocate resources accordingly. This ensures that each application is onboarded efficiently, with the appropriate security policies.

APPLICATION ONBOARDING WORKSHOP:

Early stakeholder engagement is vital to success. We hold workshops that involve key stakeholders from both the IT and business sides, to ensure that expectations are clear, potential roadblocks are identified early, and everyone is aligned on objectives.

APPLICATION CATEGORIZATION:

We introduced a system where we categorize applications based on their size and complexity—small, medium, or large, just like T-shirt sizes. We prioritize high-impact applications for immediate onboarding, while others are integrated more gradually.

Lifting the Scope: Managing Complexity Incrementally

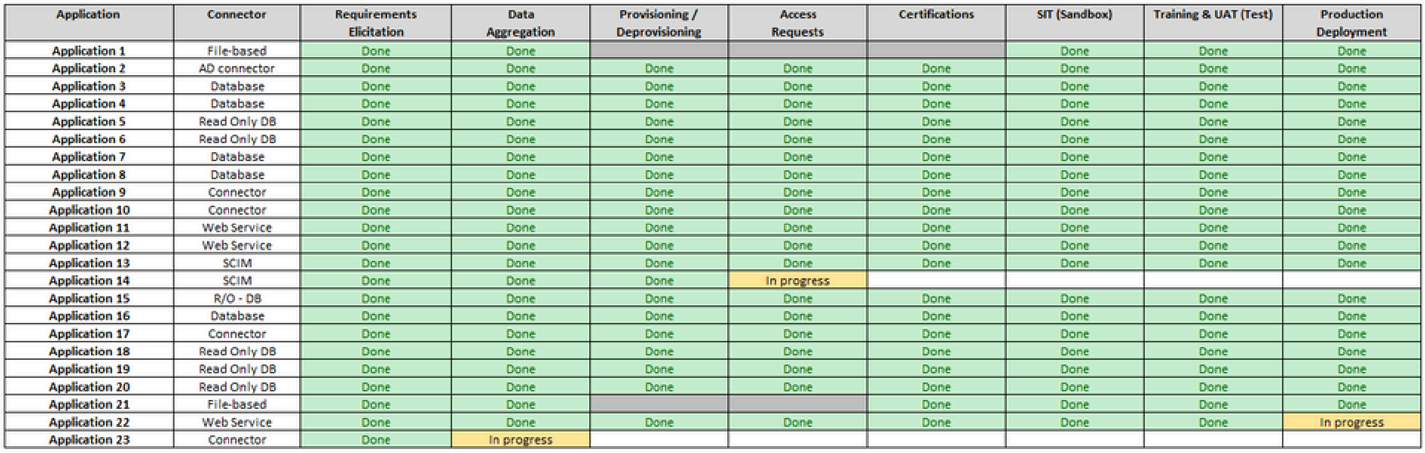
When we first started working on SailPoint implementations, we often found ourselves running into what we call “scope creep.” Essentially, trying to tackle too much at once. Over time, we realized that the best way to manage complexity is through incremental scope management or “lifting the scope”—an approach we’ve embraced in every SailPoint project.

By managing the scope of SailPoint integration incrementally, you can deliver continuous value without overwhelming the team. This method allows for constant project visibility, where stakeholders can track progress, address issues, and adjust as needed without losing momentum.

An incremental approach also ensures that any new requirements or changes in your organization’s needs can be seamlessly integrated into the existing framework without derailing the project. This flexibility is crucial, as organizations often evolve during long-term deployments, and SailPoint needs to be able to grow and adapt with them.

> Over time, we realized that the best way to manage complexity is through incremental scope management or “lifting the scope”—an approach we’ve embraced in every SailPoint project.

Progress Tracker



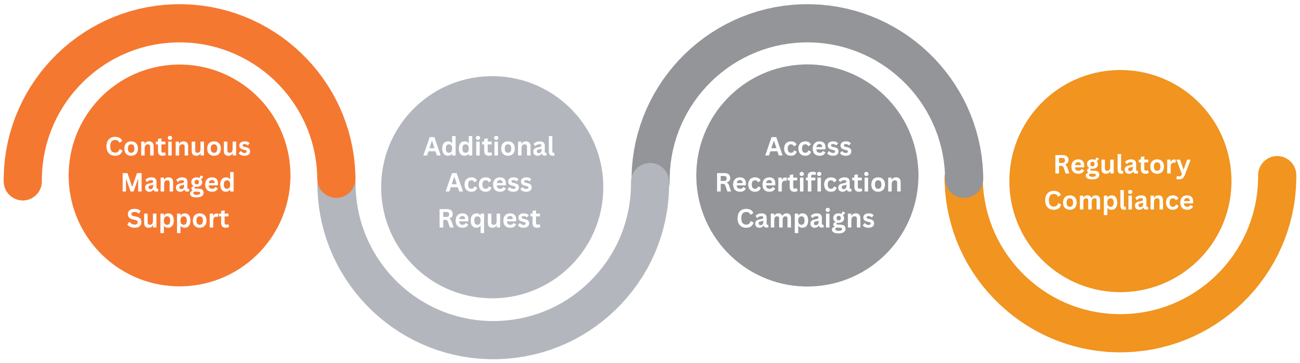
Application	Connector	Requirements Elicitation	Data Aggregation	Provisioning / Deprovisioning	Access Requests	Certifications	SIT (Sandbox)	Training & UAT (Test)	Production Deployment
Application 1	File-based	Done	Done				Done	Done	Done
Application 2	AD connector	Done	Done	Done	Done	Done	Done	Done	Done
Application 3	Database	Done	Done	Done	Done	Done	Done	Done	Done
Application 4	Database	Done	Done	Done	Done	Done	Done	Done	Done
Application 5	Read Only DB	Done	Done	Done	Done	Done	Done	Done	Done
Application 6	Read Only DB	Done	Done	Done	Done	Done	Done	Done	Done
Application 7	Database	Done	Done	Done	Done	Done	Done	Done	Done
Application 8	Database	Done	Done	Done	Done	Done	Done	Done	Done
Application 9	Connector	Done	Done	Done	Done	Done	Done	Done	Done
Application 10	Connector	Done	Done	Done	Done	Done	Done	Done	Done
Application 11	Web Service	Done	Done	Done	Done	Done	Done	Done	Done
Application 12	Web Service	Done	Done	Done	Done	Done	Done	Done	Done
Application 13	SCIM	Done	Done	Done	Done	Done	Done	Done	Done
Application 14	SCIM	Done	Done	Done	In progress				
Application 15	R/O - DB	Done	Done	Done	Done	Done	Done	Done	Done
Application 16	Database	Done	Done	Done	Done	Done	Done	Done	Done
Application 17	Connector	Done	Done	Done	Done	Done	Done	Done	Done
Application 18	Read Only DB	Done	Done	Done	Done	Done	Done	Done	Done
Application 19	Read Only DB	Done	Done	Done	Done	Done	Done	Done	Done
Application 20	Read Only DB	Done	Done	Done	Done	Done	Done	Done	Done
Application 21	File-based	Done	Done			Done	Done	Done	Done
Application 22	Web Service	Done	Done	Done	Done	Done	Done	Done	In progress
Application 23	Connector	Done	In progress						

Testing, Training, and Adoption: Ensuring Success Post-Deployment

We view testing as one of the most critical phases in any SailPoint integration. For us, it’s not just about ticking boxes—it’s about ensuring the system functions smoothly and meets all expectations before it goes live. We believe in running regular, iterative testing cycles to catch any potential issues early, long before they can affect end-users.

And we make sure to involve those end-users in the process, ensuring the solution isn’t just technically sound, but also intuitive and user-friendly. After all, it’s one thing for the system to work perfectly on paper, and another for the people using it every day to feel comfortable and confident with it.

Increased Adoption


Continuous Managed Support
Additional Access Request
Access Recertification Campaigns
Regulatory Compliance

But testing is just the beginning. Training and adoption are what truly guarantee the long-term success of any implementation. We know that the more familiar users are with the system, the more confident they'll be in using it. That's why we offer comprehensive training sessions for everyone, from IT administrators to end-users. Our goal is to empower each person to use the system effectively and troubleshoot when needed.

We don't stop at initial training either—regular refresher courses help users stay up to date with system changes and evolving business needs.

By fostering early and continuous adoption, we also help improve data security and compliance. Well-trained users are less likely to make mistakes that could compromise sensitive data or violate compliance regulations.

A Roadmap to Success

Integrating SailPoint into your organization's IAM framework is a significant undertaking, but with the right strategies in place, it can be a smooth and efficient process. By focusing on governance, fostering stakeholder collaboration, structuring the application onboarding process, managing scope incrementally, and investing in continuous training, we've been able to deliver successful SailPoint integrations time and again.

SailPoint integration is not just about deploying new technology—it's about building a secure, scalable, and adaptable identity management framework that grows with your organization's needs. When done right, it delivers lasting value, enhances security, and supports organizational objectives well into the future.

Feature

BEYOND COMPLIANCE: LEVERAGING AI IN VAPT TO IDENTIFY AND MITIGATE EMERGING SECURITY RISKS

- RAJESH MITTAL

Navigating the cybersecurity landscape can feel like an endless pursuit, just as you think you've addressed one threat, a new and evolved danger emerges. This challenge is compounded by the fact that regulatory compliance, while crucial, often fails to encompass the full spectrum of modern cyber threats. To stay ahead of this constantly evolving risk landscape, businesses need to look beyond these frameworks and leverage the power of advanced technologies, like Artificial Intelligence (AI), in their Vulnerability Assessment and Penetration Testing (VAPT) strategies. Let’s explore how AI-enhanced VAPT not only helps identify hidden vulnerabilities but also offers smarter ways to mitigate future threats proactively.

The Compliance Conundrum

Regulatory frameworks such as GDPR, HIPAA, and PCI-DSS establish a baseline for security. However, their primary focus is on meeting minimum requirements, rather than keeping pace with the rapidly evolving threat landscape. These standards can quickly become outdated as new technologies—such as cloud computing, Internet of Things (IoT) devices, and advanced social engineering tactics—emerge and proliferate. Relying solely on compliance can leave organizations vulnerable to zero-day exploits and sophisticated attack vectors that circumvent traditional defenses. This is where an AI-driven VAPT approach becomes indispensable.

The Power of AI in VAPT

AI acts as a security multiplier— transforming VAPT from a reactive exercise to a proactive safeguard. Traditionally, VAPT involves a mix of manual and automated testing to find known vulnerabilities. But AI takes things up a notch by analyzing vast amounts of data, uncovering hidden patterns, and forecasting emerging threats before they become a problem.

Smarter Vulnerability Detection:

AI tools can also be leveraged for automated code analysis, employing machine learning models to identify potential vulnerabilities, such as SQL injection, cross-site scripting (XSS), and insecure deserialization, within the application's source code. By continuously learning from vast datasets of known vulnerabilities and secure coding practices, these AI models can detect intricate patterns and subtle flaws that might be overlooked by traditional static code analysis tools or manual code reviews.

AI tools scan for vulnerabilities more quickly and accurately. They learn from data and adjust their detection methods over time, spotting issues that older methods might miss. AI can simulate how advanced threats will behave, making your security assessments much more effective. Imagine an AI tool that automatically scans cloud applications, identifying subtle misconfigurations that expose data to risk—something that might go unnoticed during manual assessments.

Adaptive Penetration Testing:

AI enhances penetration testing by evolving with current attack strategies. It automates and refines attack simulations, ensuring that your security tests stay relevant against the latest threats. Whether it’s malware, phishing, or other attack vectors, AI helps you stay ahead of cybercriminals. For instance, if malware is detected, AI can automatically replicate the malware’s tactics to see how far it can penetrate your systems, and adjust future tests based on the outcomes.

AI can also be leveraged to conduct intelligent fuzzing, a technique used to identify software vulnerabilities by sending unexpected or malformed data inputs to applications and systems. Traditional fuzzing methods often rely on predefined rules or random input generation, which can be inefficient or miss complex vulnerabilities. AI-powered fuzzing, on the other hand, can analyse and learn from the application's behavior, dynamically adjusting the input data and testing strategies to more effectively uncover vulnerabilities, such as buffer overflows, denial-of-service (DoS) vulnerabilities, or logic flaws.

Proactive Threat Monitoring:

AI continuously monitors various sources for potential zero-day vulnerabilities and exploits. By analyzing data using natural language processing and machine learning, it can quickly identify and flag new threats. This information is used to automatically update threat models and generate alerts for immediate action. AI provides detailed analysis, impact assessment, and recommends tailored mitigation steps before widespread exploitation occurs.

AI's ability to process and analyze massive amounts of data is a game-changer. As threats appear rapidly, AI helps by constantly updating threat models with real-time data. This means your organization can react to new risks almost immediately, boosting your overall security. AI also improves the response to identified threats by recommending the best actions based on past data and current system conditions, ensuring that your fixes are timely and effective.

What Do We Do Differently at Avancer?

At Avancer, we recognize that compliance is just the starting point. With over 20 years of cybersecurity expertise, we combine experience with AI-driven VAPT tools. Our AI-powered methodology holistically assesses your security posture, detecting hidden vulnerabilities, simulating advanced threats, and offering proactive mitigation strategies.

Our VAPT Evaluation Methodology:

We offer a comprehensive approach to VAPT, focusing on the following key areas:

1 ASSESSMENT OF ATTACKS:

We assess the external attack surface using AI-driven tools to scan for vulnerabilities in internet-facing servers, applications, and IP addresses, then simulate exploitation to evaluate their severity and impact.

2 IMPACT ANALYSIS OF SECURITY BREACHES:

We assess the risks of unauthorized access and the potential impact on data confidentiality, system integrity, and service availability, including the effects of data breaches or operational disruptions.

3 RISK PRIORITIZATION:

Using a composite risk score, we prioritize vulnerabilities based on exposure, severity, and exploitability, helping you address immediate threats while planning long-term improvements.

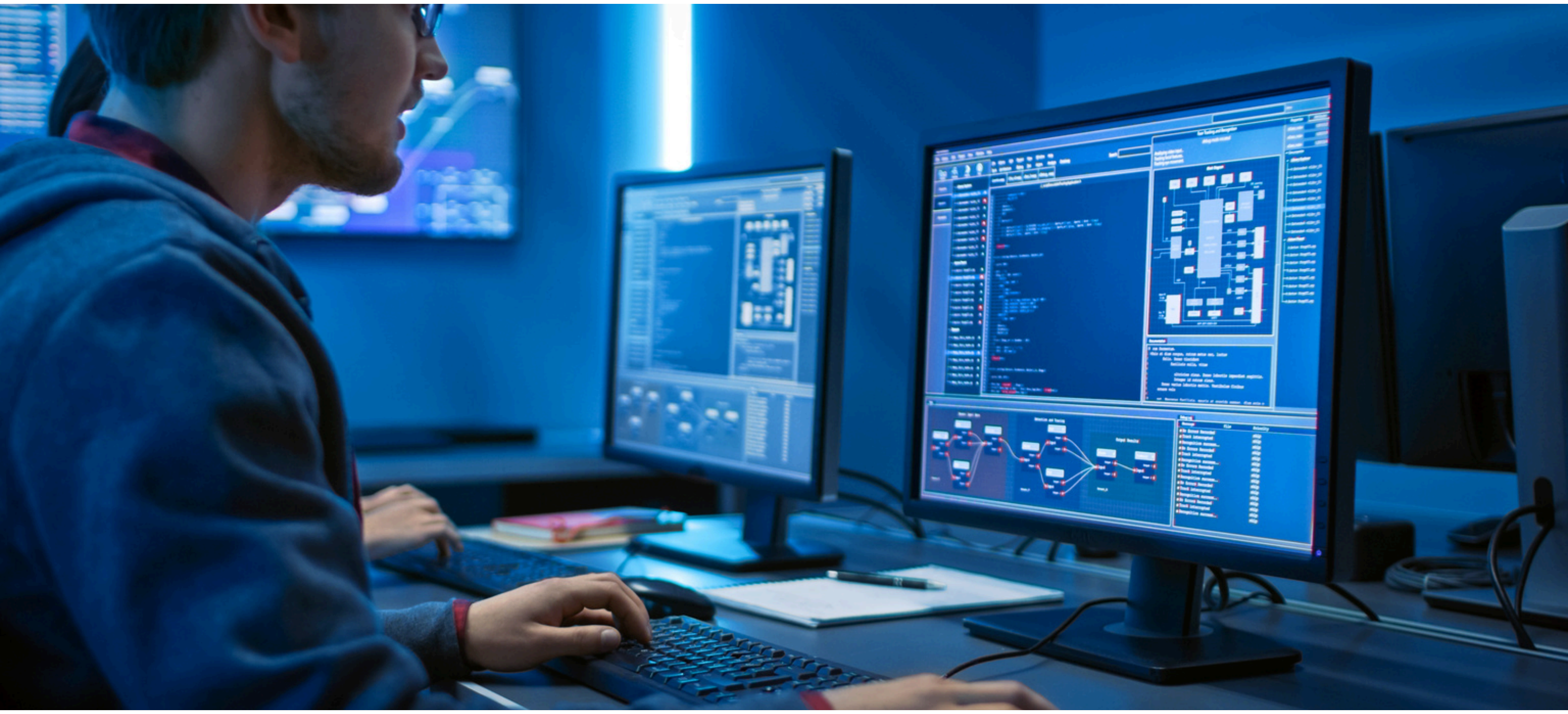
Categorizing Risks:

Our methodology categorizes vulnerabilities across multiple areas, including:

Access Controls	Issues related to user authorization and access rights.
Auditing and Logging	Gaps in action auditing and error logging
Encryption	Weaknesses in data encryption and protection mechanisms.
Data Exposure	Risks associated with the unintended exposure of sensitive information.

Meeting compliance standards is just the start. To effectively tackle today's fast-moving cyber threats, integrating AI into your VAPT strategy is essential. AI helps you uncover hidden vulnerabilities, simulate advanced attacks, and adapt your security measures to keep up with evolving threats. Leverage our AI-driven VAPT solutions to elevate your security posture and stay ahead of emerging cyber risks.

Let's transform your cybersecurity strategy together!



Cover Story

ADVANCING ACCESS CONTROL: HARNESSING AI FOR RBAC OPTIMIZATION

As cyber threats escalate and data breaches become increasingly frequent, organizations are under immense pressure to protect sensitive information. Role-Based Access Control (RBAC) has been a fundamental approach to managing access rights, assigning permissions based on roles within an organization. However, traditional RBAC systems often face challenges in keeping pace with the growing complexity of IT environments. These limitations can lead to inefficiencies, reduced adaptability, and potential security vulnerabilities.

This is where Artificial Intelligence (AI) emerges as a game-changer. By integrating AI into RBAC systems, organizations can unlock transformative capabilities that redefine access control. AI enhances traditional methods by automating role assignments, analyzing access patterns, and proactively adapting to changes in organizational structures. This not only improves efficiency but also strengthens security, ensuring access policies remain precise and aligned with evolving business needs.

The Current Landscape of RBAC

RBAC's strength lies in its structured approach—granting access according to job functions. Yet, as businesses expand and evolve, this structure can become challenging. Some of the key issues are discussed below.

Key Challenges in Legacy RBAC Frameworks

INEFFICIENCIES: 1

Manual processes for role assignment and access management can be time-consuming and prone to error. A report by **IBM indicates that 22 per cent of data breaches are caused by human error**, often due to misconfigured access controls.

SECURITY RISKS: 2

Outdated roles can leave organizations vulnerable to unauthorized access, and poorly defined roles can lead to excessive permissions. The **Verizon Data Breach Investigations Report notes that 30 per cent of breaches involved internal actors**, highlighting the need for precise access management.

COMPLIANCE CHALLENGES: 3

Ensuring compliance with regulations such as GDPR, HIPAA, and SOX becomes increasingly challenging with static RBAC systems that cannot adapt to changing business needs. **Non-compliance can result in hefty fines**—GDPR, for example, can impose penalties of up to Euro 20 million or 4 per cent of annual global turnover, whichever is higher.

The Role of AI in RBAC Optimization

By automating role assignments and access requests, AI reduces friction in the user experience, allowing employees to focus on their core responsibilities without delays.

Robert Byrne, Field Strategist at OneIdentity, emphasizes the importance of integrating AI insights into existing identity and access management systems. *"The key to integrating AI recommendations for RBAC into existing IAM workflows is to target the right persona with the proper AI insight. For example, line managers care about ease of access for their teams, so they welcome role recommendations at the team level. We need to surface role evolution recommendations for role owners because that's what they struggle with each day. Compliance officers appreciate insights into contradictory or emerging SOD patterns in the RBAC dataset,"* he explains. *"Targeting the right persona to receive AI insights for RBAC allows us to delegate access decisions to individuals with enough motivation and knowledge to use those insights well. This means we have better engagement from the business with IAM, more accurate and timely access decision-making, and an overall improvement in security posture,"* Byrne further adds.

AI can identify and mitigate potential risks by analyzing patterns that humans might miss, thus strengthening the overall security framework. For instance, organizations that implement AI-driven monitoring can detect anomalies in user behavior that may indicate potential insider threats, addressing security risks more effectively.

> "In this complex landscape, AI offers transformative capabilities, enhancing RBAC systems through advanced optimization techniques that promise improved scalability, accuracy, and security."

Machine Learning: Transforming Static RBAC into Dynamic Systems

Traditional RBAC systems have long struggled with adaptability, particularly in fast-changing business environments such as mergers, acquisitions, or shifts in strategy. During these transitions, role definitions often need to be overhauled, a process that can be manual, slow, and prone to errors. Static frameworks tend to leave organizations vulnerable, as access rights are not flexible enough to accommodate these changes in real time.

AI-powered machine learning emerges as a transformative force at this juncture. Machine learning algorithms can sift through massive volumes of access data to identify patterns, detect anomalies, and flag potential risks. **With AI, RBAC systems can continuously learn from user behavior, dynamically adjusting access rights as roles evolve.** For instance, if an employee's activities deviate from typical behavior, machine learning models can automatically trigger reviews or adjust permissions to mitigate security risks. A study by McKinsey highlighted that companies utilizing AI for access management have achieved a remarkable reduction in security incidents, with reductions reported between 60 per cent to 80 per cent. This significant improvement underscores AI's role in enhancing security measures and streamlining access control processes within organizations.

Predictive Analytics: Proactive Role Assignments for Future-Proofed Access

As organizations scale, their role hierarchies and associated permissions grow in complexity, often resulting in role overlap and confusion. Traditional access management systems are often reactive, assigning permissions after changes occur, which can lead to security gaps and inefficiencies.

Predictive analytics changes this approach by allowing organizations to anticipate and plan for future access needs based on historical data. **By analyzing patterns in user activity, AI-powered predictive models can recommend access rights before they become necessary, aligning with real-time business demands.** This proactive method ensures that access permissions are always appropriate and compliant with industry regulations. For example, under HIPAA, organizations must enforce stringent controls over patient data. AI-driven predictive analytics can ensure that access permissions are continuously updated to meet compliance standards, reducing the risk of breaches and non-compliance penalties.

Role Mining and Dynamic Role Management: Simplifying Role Complexity

One of the most daunting challenges in RBAC systems is managing role complexity, particularly as organizations expand. Over time, roles can proliferate, leading to what's known as 'role explosion'—where too many overlapping or unnecessary roles exist, creating confusion and security vulnerabilities. This is where AI-driven role mining can be an invaluable tool.

Role mining techniques automatically analyze user activities and historical data to recommend optimal role definitions and refine existing ones. Dynamic role management enables real-time adjustments to roles based on the current needs of the business and evolving user behavior. This flexibility is especially critical for maintaining compliance with regulations like SOX, which demands strict controls over financial data access. AI not only ensures that role definitions are clear and up-to-date but also helps prevent unauthorized access, improving both security and operational efficiency.

Overcoming AI Integration Challenges

Despite its promise, integrating AI into RBAC systems isn’t without challenges. One of the biggest hurdles is ensuring the **quality of identity and access data**, with AI systems relying on accurate data to make informed decisions. As **Byrne points out**, *"The main challenge in using AI for RBAC is poor-quality identity data. Nothing will scupper your AI for RBAC initiative faster than poor quality identity profile or entitlement data. Poor quality data means that AI will fail to discern structure in the data or, worse, will recommend inappropriate roles or erroneous access decisions. To avoid the garbage-in-garbage-out pitfall and maintain a high-quality identity warehouse, organizations require a robust and extensible identity governance platform with the power to integrate business, HR, and application lifecycle processes.”*

Byrne further explains, *“This ensures that the identity warehouse remains an authoritative and reliable reflection of the state of identity across the whole enterprise, maximizing your chance of successfully applying AI for RBAC.”*

> Addressing data quality concerns is paramount to ensuring that AI-driven RBAC delivers the expected benefits. Organizations must first conduct thorough assessments of their existing RBAC systems and data to ensure a smooth transition.

Future Trends in AI-Powered Access Control

As AI continues to evolve, several emerging trends are set to shape the future of access control systems:

1. **Continuous Authentication:**

   Continuous authentication leverages AI to monitor user behavior, ensuring secure and appropriate access throughout sessions while aligning with regulatory requirements for robust access controls.

2. **Self-Service Access Requests:**

   AI-driven self-service portals streamline access by enabling role-based requests, automatically approved or denied through AI analysis, ensuring compliance with standards like ISO 27001 for information security.

3. **Integration with Other Security Technologies:**

   AI-powered RBAC systems will integrate with anomaly detection and SIEM solutions, creating a comprehensive security ecosystem. Gartner predicts that by 2025, 75% of organizations will adopt an integrated approach to identity and access management.

4. **Regulatory Compliance Automation:**

   With evolving regulations, AI can help organizations maintain compliance by automating report generation, tracking access rights, and identifying violations. Automated compliance checks ease the burden on teams and ensure adherence to regulations like GDPR and PCI DSS.

AI in RBAC – A New Era of Access Control?

The fusion of AI and RBAC signals a significant leap forward for organizations looking to bolster their access control frameworks. By addressing inefficiencies, security risks, and compliance challenges, AI offers a robust solution that is adaptable, scalable, and future-proof. While there are obstacles to overcome, particularly in data management, the benefits of AI-driven access control far outweigh the challenges.

As Rajesh Mittal, CTO of Avancer, advises, *"Organizations seeking to integrate AI into their RBAC systems should start with a detailed evaluation of their current roles and identity data. By laying this groundwork, they'll be well-positioned to fully harness AI's capabilities and optimize their access management. This initial assessment is critical, as it ensures that AI can deliver meaningful insights based on accurate and complete data. Without clean and well-defined roles, AI might amplify existing inefficiencies rather than solve them. With the right foundation, however, businesses can expect not only enhanced security but also a significant boost in operational efficiency and compliance."*

With AI's continued evolution, we can expect access control to become more intelligent, proactive, and secure—paving the way for organizations to better protect their sensitive information in an increasingly digital world.

References:

- IBM Security. (2024). "Cost of a Data Breach Report 2024." https://www.ibm.com/reports/data-breach
- Verizon. (2024). "Data Breach Investigations Report." https://www.verizon.com/business/resources/reports/dbir/
- McKinsey & Company. (2024). "The state of AI in early 2024: Gen AI adoption spikes and starts to generate value." https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai

FIVE PRIVILEGED ACCESS MANAGEMENT BEST PRACTICES TO THRIVE IN THE HYBRID AND MULTI-CLOUD ERA

- ONEIDENTITY TEAM

Guest Post

The world is becoming more cloud-native every day. Infrastructure spending is estimated to rise by 19.3 per cent in 2024, partly driven by 'new and existing mission-critical workloads.' Investment and innovation is going hand-in-hand, as new and established businesses race to modernize architecture and provision applications. At the same time, many are demanding hyperscale and high-performance cloud providers to run AI and machine learning services.

Consumers of these new models, from monolithic institutions down to end users, have one thing in common: they expect agility, portability and freedom of choice. That's why organizations are increasingly opting for multi-cloud and hybrid cloud strategies. By combining and unifying on-premises and cloud, organizations can mix and match to suit their needs. That's the goal – until you run into the age-old question of interoperability.

Different cloud services have their own sets of roles, permissions and privileges, some that come secure-by-design, and others requiring degrees of hardening.

Organizations need proven ways to ensure privileged access can be managed without sprawl, increasing consistency while also boosting efficiency. Otherwise, scalability and visibility remain limited, while the attack surface expands. To achieve this reality with PAM for cloud, we recommend starting with the following five PAM best practices.

1. Centralized visibility and control

PAM in hybrid and multi-cloud environments is dynamic, and so requires a simplified and centralized solution. Correct configuration leads to advantages such as being able to record SaaS application usage to build logs for auditing and analyzing events, actions and activities. Also being able to record user sessions, isolating specific users when you want to limit lateral movement and prevent unauthorized access.

A single pane of glass becomes the focal point for implementing Role-Based Access Control (RBAC) and integrating with Microsoft Entra ID. It's then easier to secure with auto-login through credential injection. Local server account passwords can be vaulted centrally, to be deployed and rotated in real-time, rather than kept on-premises with local deployment on one device at a time.

The reduced manual input makes it easier to scale with fewer resources, in terms of both hardware and human labor. Plus, managing access from one location helps minimize the inconsistencies and potential errors when managing multiple dashboards, each with proprietary definitions of roles to be remembered.

Predictive analytics changes this approach by allowing organizations to anticipate and plan for future access needs based on historical data.

By analyzing patterns in user activity, AI-powered predictive models can recommend access rights before they become necessary, aligning with real-time business demands. This proactive method ensures that access permissions are always appropriate and compliant with industry regulations. For example, under HIPAA, organizations must enforce stringent controls over patient data. AI-driven predictive analytics can ensure that access permissions are continuously updated to meet compliance standards, reducing the risk of breaches and non-compliance penalties.

2. Consistent policy enforcement

Securing a PAM hybrid environment doesn't happen in isolation. It calls for a unified approach across people, process and technology. Achieve visibility across these three components, and it becomes easier to manage real-time security and protection as part of the wider identity and access management strategy. The solution can then offer just-in-time (JIT) access for privileged accounts, with systems and networks segmented. Privileges can be granted at the point they're required, reducing exposure to risks from perpetual privileged access.

The time-based access controls ensure a dynamic balance of usability and security, without lengthy approvals that can bring down productivity. This becomes an enabler for enforcing the principle of Least Privilege, and an alternative to other enforcement methods such as RBAC or ABAC.

Certain elements will be repeatable, and so become potential candidates for automation. For example, canceling privileges and taking actions when malicious behavior is detected. More routine activities can include predefining access rules, allowing faster self-service access at scale. Reducing the reliance on manual approvals results in a reduced risk of access errors and privilege creep, a constant threat in growing enterprises where new employees and newly merged departments are common.

3. Adopting Zero Trust architecture

Hybrid and multi-cloud are outside the traditional perimeter – a place of remote users, threats from BYOD and a security model of 'never trust, always verify'. By default, all network devices are regarded as potential threats, and require constant verification to stay connected. The Zero Trust model is designed for this complex business environment, where no clear edge means the protective focus is on individual users, assets and resources.

> Identity is key to successful hybrid and multi-cloud-based Zero Trust implementation. Configuring means there can be fine-grained policies and rulesets for devices, with separate versions for applications

NIST SP 800-207 sets out Zero Trust principles as a set "for workflow, system design and operations that can be used to improve the security posture of any classification or sensitivity level."

The distributed nature of cloud means users need to connect from anywhere – with least-privilege access authorized and encrypted. MFA turns cloud-based complexity into a security strength, because it's less likely an attacker will be able to access all authentication factors at once. Implementation can go beyond simply granting privileged access based on a specific factor. For example, adding granularity to validate the factor only at specific times or geolocations. Plus, there's improved user experience for genuine first-time logins, with no need to repeatedly produce all authentication factors.

Identity is key to successful hybrid and multi-cloud-based Zero Trust implementation. Configuring means there can be fine-grained policies and rulesets for devices, with separate versions for applications. This allows teams to add more context to approval paths, including relevant mechanisms and alerts for anomalies, unusual behaviors and intrusion detections. Here's where a protocol such as multi-factor authentication (MFA) is an integral part of hardening the security posture.

Zero Trust architecture Covers:

Locations and devices: 1 — "Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location."

Sessions: 2 — "Authentication and authorization (both subject and device) are discrete functions performed before a session to an enterprise resource is established."

Resources: 3 — "Protecting assets, services, workflows and networks accounts because the network location is no longer seen as the prime component to the security posture of the resource."

4. Regular auditing and compliance

Alongside security and Zero Trust, further drivers come from compliance and governance. There's the rise in 'cloud sovereignty', where government agencies will need to meet strict requirements around data localization and access. For hybrid and multi-cloud environments, this means understanding where and how data is collected and stored, ensuring processes comply with the relevant jurisdiction and industry requirements. One example is HIPAA's Security Rule in relation to access controls, where "rights and/or privileges should be granted to authorized users based on a set of access rules that the covered entity is required to implement."

Of course, as cloud evolves so does the definition of 'user'. Organizations have to manage privileged access for hybrid and multiple forms of devices and applications. These entities require their own identities, much like human employees. Of course, unlike human employees, these machine identities can't simply hand in their credentials and exit the building when it's time to depart. Instead, the solution is to implement robust Identity Lifecycle Management to support compliance and auditing. This gives visibility of all entities, and allows automated provisioning and deprovisioning, even for elevated privileges, at scale.

5.Training and awareness

Training and awareness are essential – with rationale to explain why and encourage buy-in, rather than simply "do this, and don't do that." For example, educating staff to be aware of the Separation of Duties concept, and how compliance is why they may need to approve, or wait to be approved, access to resources. This can also be extended to admins, making sure there is segregation between who assigns and who receives privileged access.

For a topic framework accessible to non-technical audiences, look no further than Gartner's four pillars of PAM:

1 Track and secure every privileged account:

Tracking needs to be continuous, to mitigate attackers that only need to be lucky once

2 Govern and control access:

Lifecycle management is business-critical, with JIT the recommended method of ensuring no standing privileged access

3 Record and audit privileged activity:

Gain visibility into what privileged users are doing or changing

4 Operationalize privileged tasks:

This pillar highlights the importance of automation. For DevOps and RPA initiatives, delegating privileged access, plus predictable and repeatable tasks, configurations, and installations

By raising security awareness across these pillars of PAM, organizations can ensure the right balance between enabling access, mitigating risks and minimizing friction.

Cloud migration and PAM migration: Leading the way with a hybrid approach

The cloud enables businesses to enter the future. At the same time, many of these businesses were built in the past. That's why a hybrid approach, for a 'best of all worlds' strategy, is often the way to go. It's also why, "efforts to modernize will likely carry on for another five to 10 years," according to Forrester. A PAM solution that allows this more composable approach will be business-critical for both strategic and security reasons.

Threat actors are all too aware of the gaps that can be exploited, with the CISA and NDA highlighting default configurations and improper separation of user/administrator privileges as the two most common systemic weaknesses in many large organizations, including those with mature cyber postures. This impacts everyone from IT security and operations, to DevOps and compliance, through to business leaders and decision-makers. In fact, it impacts anyone within an enterprise that needs access to an application, service or system.

Following the best practices above are a step towards successful PAM. It starts with centralizing processes, for consistent control across cloud environments. The resulting foundation provides the platform for enforcing policies and introducing or accelerating automation. Of course, that is, as long as automation comes with the strict controls for adopting Zero Trust architecture.

The continuous monitoring and adaptive controls secure the business and create an auditable trail to satisfy compliance and regulatory requirements. An added protective layer comes from equipping human workers with PAM expertise, educating and training. Combining these best practices means enhanced security for hybrid and multi-cloud environments, with the flexibility, scalability and visibility that's needed for PAM. By now you may be wondering about next steps for PAM in hybrid and multi-cloud. You can get started with a free trial of our PAM solutions.

References:

- IDC Research. (2024). "Spending on Shared Cloud Infrastructure Continues to Lead the Way in Enterprise Infrastructure Investments, According to IDC Tracker" https://www.idc.com/getdoc.jsp?containerId=prUS52001524
- NIST. "NIST SP 800-207 Zero Trust Architecture." https://csrc.nist.gov/pubs/sp/800/207/final
- Gartner. (2021). "The 4 Pillars of Privileged Access Management." https://www.gartner.com/smarterwithgartner/the-4-pillars-of-privileged-access-management
- CISA. (2023). "NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations." https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-278a
- OneIdentity. https://www.oneidentity.com/trials/#bysolutionprivilegedaccessmanagement

Guest Post

CIAM: FOSTERING COMPLIANCE, BUILDING TRUST

- AMMAR FAHEEM, PRODUCT MARKETING MANAGER, THALES

The advent of regulations like GDPR and CCPA/CPRA has empowered individuals with unprecedented control over their personal data. This has presented organizations with numerous challenges when it comes to managing and complying with an ever-increasing set of global data privacy regulations.

This has also raised customer expectations around self-service capabilities when it comes to their data privacy, consents, and preferences.

Customer Identity and Access Management (CIAM) solutions offer a strategic approach to addressing these challenges. By centralizing customer identity data and automating data handling processes, CIAM significantly improves efficiency and compliance. Gone are the days of labor-intensive manual processing, prone to errors and delays. CIAM streamlines data management, reducing operational costs and minimizing the risk of human error.

Beyond efficiency, CIAM is a cornerstone of robust security. By supporting an Identity centric security posture as your first line of defense, CIAM solutions ensure customer data is handled securely, minimizing the risks of data breaches. Moreover, CIAM empowers customers with self-service capabilities, allowing them to manage their data directly, aligning with the principles of data ownership and control.

The strategic benefits of CIAM extend beyond compliance. Modern CIAM solutions have features that address compliance needs and align with strategic business objectives. Key features include:

Key Features of Modern CIAM

1 User-Centric Design:

Through intuitive user interfaces, CIAM solutions make it easier for customers to manage their personal data. This user-centric approach enhances the customer experience, fostering loyalty and trust.

2 Automated Data Processing:

Automation is at the heart of CIAM solutions, facilitating swift and accurate handling of data requests. This feature significantly reduces the time and resources required for data management.

3 Robust Security Measures:

Security is paramount in CIAM solutions. Features like multi-factor authentication, encryption, and regular security audits ensure that personal data is protected against breaches, maintaining compliance and safeguarding reputation.

4 Scalability and Flexibility:

As businesses grow, CIAM platforms can scale accordingly. This flexibility ensures that companies can adapt to increasing data volumes and evolving regulatory landscapes without compromising efficiency or compliance.

5 Integration Capabilities:

Modern CIAM solutions are designed to integrate with existing business systems and technologies seamlessly. This integration capability ensures a unified approach to data management across various platforms and services.

6 Analytics and Reporting:

Advanced analytics and reporting features provide insights into user behavior and data management trends. These insights are crucial for strategic decision-making and continuous improvement of data practices.

As data privacy regulations continue to evolve, modern CIAM tools are becoming increasingly critical for organizations seeking to protect customer data while maintaining operational efficiency. Through a robust CIAM solution, businesses can not only meet regulatory requirements but also gain a competitive advantage through improved customer relationships and operational excellence.

AVANCER EXPANDS ITS IDENTITY & ACCESS MANAGEMENT SERVICES TO CUSTOMER IDENTITY & ACCESS MANAGEMENT (CIAM) WITH THALES

Avancer, a leading IAM Systems integrator, announces a collaboration with Thales, a global technology provider in digital identity and security, to advance its business in the growing IAM market. As part of the agreement, Avancer will offer Thales' advanced Customer Identity and Access Management (CIAM) solutions as a reseller and implementation partner, providing organizations with the tools to fortify security, ensure compliance, and enhance customer digital experiences.

Connecting customers and partners with applications and data needs to be frictionless and secure. These external users usually outnumber the internal users. Organizations are increasingly threatened by data breaches and cyberattacks, therefore a robust CIAM solution is no longer optional—it is essential. The collaboration between Avancer and Thales harnesses the strengths of both companies, combining Avancer's deep expertise in IAM with Thales' innovative technology to address the evolving challenges of digital identity management. This collaboration also aligns with Avancer's strategic vision to expand its solution portfolio, penetrate new markets, and deliver unparalleled value to clients in North America.

> “The collaboration with Thales allows us to expand our offerings and provide our clients with world-class CIAM solutions that address the growing complexities of digital identity management. Together, we are setting a new standard for secure and seamless customer experiences,” **said Rajesh Mittal, CTO at Avancer.** ”

Key Highlights of the Partnership:

- Comprehensive CIAM Solutions: Avancer will offer the full suite of Thales' CIAM products to orchestrate B2C and B2B use cases, including identity verification, passwordless authentication, and delegated administration, tailored to meet the unique needs of enterprises across various sectors
- Seamless Implementation: Leveraging Avancer's extensive experience in IAM, customers will benefit from a seamless and efficient implementation process, ensuring that Thales' CIAM solutions are integrated smoothly into their existing systems.
- Regulatory Compliance: The partnership emphasizes compliance with global regulations such as HIPAA, GDPR, CCPA, and other data protection standards, providing clients with the assurance they need in an increasingly regulated environment.

Maarten Stultjens, VP CIAM for the Americas at Thales added

> “Every business is different. Avancer can help these businesses to get the best out of our CIAM technology, create awesome customer journeys to increase revenue and reduce IT-risks. So we are extremely excited to collaborate with the Avancer experts in North America. ”

SECURING PATIENT DATA IN THE ERA OF DIGITAL AGE

- GIRISH KOPPAR, GM-IT,
WOCKHARDT HOSPITALS

In the digital age, patient data is vulnerable to attacks and healthcare providers face unprecedented challenges in securing it. The shift towards digital health records, telemedicine, and health information exchanges has revolutionized the efficiency and accessibility of healthcare. However, these advancements also bring significant risks regarding data security and patient privacy. Protecting patient data is not only a regulatory requirement but also a fundamental aspect of maintaining trust between healthcare providers and patients. This article outlines the key strategies and practices for safeguarding patient data in the digital era.

Regulatory Landscape

Healthcare organizations need to comply with lots of local and international regulatory standards to protect patient data. Key regulations include:

Health Insurance Portability and Accountability Act (HIPAA):

In the United States, HIPAA sets the standard for protecting sensitive patient information. Compliance requires healthcare providers to implement administrative, physical, and technical safeguards.

General Data Protection Regulation (GDPR):

For organizations operating in the European Union, GDPR imposes stringent data protection and privacy requirements. This regulation mandates robust data protection measures and grants patients extensive rights over their data.

National and Regional Regulations:

Various countries and regions have their own regulations and standards for patient data protection, such as the Personal Data Protection Act (PDPA) in Singapore and the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada.

DPDP Act (Digital Personal Data Protection Act)

The DPDP Act governs processing of digital personal data in India. It applies to data collected online or offline and digitized. The Act extends to entities outside India if they process personal data for offering goods or services in India.

Key Strategies for Protecting Patient Data

1. Data Encryption: Encrypting patient data both at rest and in transit is essential to prevent unauthorized access. Advanced encryption standards (AES) and secure socket layer (SSL) protocols ensure data is protected during storage and transmission.

2. Access Controls and Identity Management: Implementing strict access controls ensures that only authorized personnel can access sensitive patient information. Role-based access control (RBAC) limits data access based on the user’s role within the organization. Multi-factor authentication (MFA) adds an extra layer of security by requiring additional verification.

3. Regular Audits and Monitoring: Conducting regular audits and monitoring data access logs helps detect and respond to suspicious activities. Automated monitoring tools can identify unusual patterns and potential breaches in real time.

4. Data Minimization: Collecting and retaining only the minimum necessary patient data reduces the risk of exposure. Data minimization involves identifying and eliminating redundant or obsolete information from the system.

5. Employee Training and Awareness: Human error is a significant factor in data breaches. Regular training and awareness programs ensure that employees understand their responsibilities in safeguarding patient data. Phishing simulations and cybersecurity drills can help prepare staff for potential threats.

6. Data Anonymization and Pseudonymization: Anonymizing or pseudonymizing patient data where possible reduces the risk associated with data breaches. These techniques involve removing or obscuring personal identifiers, making it difficult to trace the data back to individual patients.

7. Incident Response Plan: Developing and regularly updating an incident response plan is crucial for addressing data breaches swiftly and effectively. This plan should outline steps for containing the breach, notifying affected patients, and complying with regulatory reporting requirements.

8. Vendor Management: Healthcare organizations often rely on third-party vendors for various services, such as cloud storage and data processing. It is essential to ensure that these vendors comply with data protection regulations and implement robust security measures. Regular assessments and audits of vendor practices are necessary to maintain data security.

Key Strategies for Protecting Patient Data

1. Electronic Health Records (EHR) Systems: Modern EHR systems come with built-in security features, such as audit trails, access controls, and encryption. Choosing a reputable EHR vendor and keeping the system updated with the latest security patches is critical.

2. Blockchain Technology: Blockchain offers a decentralized and tamper-proof way of storing patient data. By providing a secure and transparent ledger, blockchain can enhance data integrity and reduce the risk of unauthorized access.

3. Artificial Intelligence and Machine Learning: AI and machine learning can enhance data security by identifying and responding to threats in real-time. These technologies can analyze large volumes of data to detect anomalies and potential security breaches.

Challenges and Considerations

1. Balancing Accessibility and Security: Ensuring that patient data is accessible to healthcare providers while maintaining strict security measures can be challenging. Striking the right balance is crucial for delivering quality care without compromising data protection.

2. Evolving Threat Landscape: Cyber threats are constantly evolving, and healthcare organizations must stay ahead of emerging risks. Regularly updating security protocols and investing in advanced cybersecurity solutions are essential for staying protected.

3. Patient Trust and Engagement: Maintaining patient trust is paramount. Transparent communication about data protection measures and respecting patient privacy rights contribute to a trustworthy healthcare environment.

Regulatory Insights

ENSURING DPDP ACT COMPLIANCE WITH IDENTITY & ACCESS MANAGEMENT (IAM)

The **Digital Personal Data Protection (DPDP) Act, India**, establishes a robust regulatory framework to **safeguard personal data**, ensuring transparency, accountability, and security. As part of a global shift towards stricter data protection laws, this legislation brings India in line with international privacy standards. With data breaches and privacy concerns on the rise, businesses operating in India must implement advanced **security measures such as Identity & Access Management (IAM) solutions** to align with the Act's requirements.

Overview of the DPDP Act

01 Data Security and Privacy:

Organizations must safeguard personal data against unauthorized access, misuse, and breaches.

02 Accountability:

Clear responsibilities for data controllers and processors to ensure compliance.

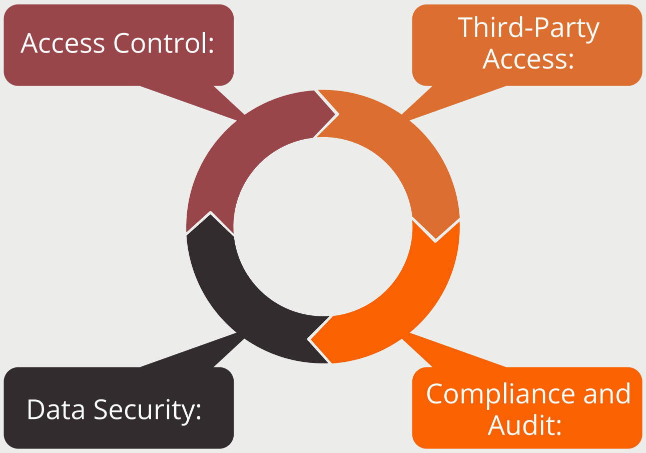
03 Transparency and Consent:

Individuals' rights to know how their data is used and to provide informed consent.

04 Breach Notification:

Obligations to report breaches promptly and mitigate risks.

Implementing Identity and Access Management (IAM) is crucial for complying with DPDP Act. Here's how IAM contributes:



Access Control:

IAM restricts data access based on user roles, ensuring individuals access only necessary information, thereby enforcing the principle of least privilege.

Third-Party Access:

IAM enforces adaptive authentication and granular access controls for external vendors, ensuring secure data handling in compliance with the DPDP Act.

Data Security:

By monitoring user activities and automating credential management, IAM helps detect and prevent unauthorized access, enhancing overall data security.

Compliance and Audit:

IAM maintains detailed access logs and audit trails, simplifying regulatory reporting and demonstrating adherence to the DPDP Act.

Avancer offers vendor-agnostic IAM solutions to help organizations navigate DPDP Act compliance, ensuring your business meets regulatory requirements while safeguarding sensitive data.

Data Governance for a Leading Indian Public Undertaking Bank

Highlights

We successfully executed a data governance project in the financial and banking sector, utilizing SyberGRC, an advanced data scanning product. Our implementation involved scanning diverse file types to identify and manage privacy data across 140 machines. As system integrators and application integrators, we played a pivotal role in implementing the solution and providing ongoing support to ensure seamless operation and compliance with industry standards.

Executive Summary

A leading Indian Public Sector Undertaking (PSU) Bank, for its Chicago branch, engaged Avancer Corporation to conduct a Data Assessment and Scan on assigned hosts/machines containing sensitive information to investigate the entire universe of their data.

- **Data Scanning:** Identified confidential data, including PII, PHI, PCI, and other business-sensitive information stored in laptops and desktops.
- **Data Remediation:** Developed an action plan to protect data from exfiltration.

CHALLENGES

- To identify confidential data that included PII, PHI, PCI, and other business confidential data stored in laptops and desktops.
- To perform secure scans across various file types, conducting in-depth data analysis, and providing a comprehensive recommendation plan to enhance data security.

BENEFITS

- **Enhanced Data Identification:** Enabled the identification of critical or sensitive customer data, restricted access to PII, and regularly detected duplicate and stale data.
- **Effective Data Classification:** Successfully implemented data classification techniques by applying metadata tags, eliminating stale data, integrating with DLP policies, and enforcing daily access controls.
- **Improved Data Management:** Discovered and eliminated stale or redundant data, integrated classification into DLP and other policy-enforcing applications, and regulated user access to data effectively.
- **Optimized Metadata Utilization:** Enabled metadata tagging to enhance business operations, track data location and usage, and uncover valuable trends.

KEY TECHNOLOGIES

- SyberGRC Data Scan, Active Directory, SAN storage, laptops/servers

AVANCER'S SOLUTION

- Deployed an advanced scan product for L1 file types and an L2 data scanner.
- Enabled seamless identification of data stored across the environment.
- Continuously reapplied privacy metrics based on the sensitivity of collected and identified data.
- Generated automated system reports displaying additional confidential data in the environment.
- Provided strategic recommendations to enhance data security.

> **Deployed advanced scanners to identify, classify, and securely protect data.**

Enhancing Healthcare EMR: Seamless Integration and Automated Identity Lifecycle with Identity Bridge

Highlights

We successfully deployed Identity Bridge as a tailored IAM solution in a healthcare company, seamlessly integrating it with the client's existing systems, including their Healthcare EMR system, to manage 34,000 identities securely. We ensured seamless deployment and provided ongoing support for optimal performance and compliance.

Executive Summary

A leading US-based healthcare provider faced challenges with user provisioning and automating account setups for their EMR system. We seamlessly integrated their on-premise identity system and deployed critical IAM modules across 28 sites, optimizing workflows, reducing manual effort, and enhancing efficiency.

CHALLENGES

- To overcome significant challenges in provisioning into the EMR system.
- To address hurdles in automating user and provider creation due to limited market solutions.
- To implement a solution for integrating the on-premise identity management system.
- To automate and streamline manual workflows for improved efficiency.

BENEFITS

- The seamless EMR integration reduced manual efforts significantly.
- Automation of complex provisioning processes resulted in a smoother workflow.
- The solution showcased Avancer’s powerful API integration capabilities.
- It offered substantial cost savings for the healthcare provider.
- The deployment approach ensured stability and reliability, addressing any bugs or issues before reaching the client’s production environment.

REVIEW & QUALITY CONTROL

- Client efficacy was primarily determined by thorough testing and client reviews.
- The product did not directly move to production but underwent rigorous testing in the client's free-broad environment.
- Weekly client feedback and internal discussions ensured ongoing improvements and customization, meeting specific requirements.
- A robust project management system and daily sprints tracked development progress and bug fixing.

AVANCER'S SOLUTION

- Avancer proposed and successfully deployed three critical modules for the client: User, Provider, and Active Directory.
- The deployment spanned 28 sites and hospitals within the healthcare organization.
- The team implemented a quality-focused approach, including a meticulous testing stage, pre-prod server deployment, and a replicated environment mirroring the client's in a Red Hat setup.
- The team adapted the Active Directory connector to meet specific requirements, introducing a declarative rule-building approach and role management based on department and job title matrices.

> **Avancer deployed key healthcare modules, optimized AD connectors, and ensured seamless integration through rigorous testing.**

AVANCER IN NEWS

avancer
Simplified IT Security
Avancer: Leading the Future of Identity Security
Your Long-Term Trusted SailPoint Partner
Our Journey
Unmatched Expertise in IIQ & ISC
Advanced Technical Skills in NERM, ARM & Data Access Sec
Strategic IAM Advisory Acumen
End-to-End SailPoint Implemen
Rapid & Tailored Application Onboa
Trusted Manageme SailPoint Solutio
Experienced SailPoint-Certifie
avancercorp.com

SailPoint Navigate 2024

Avancer Corp participated in SailPoint Navigate 2024, held from October 21-23 at the Hyatt Regency Orlando, Florida. As a Silver Sponsor, we joined industry leaders to exchange insights and advancements in identity governance. Our expert-led session, "Navigating SailPoint Integration: Tips for Smooth Implementation and Deployment," showcased our proficiency in SailPoint solutions. Further, our certified consultants presented tailored solutions for sectors like healthcare and financial services, ensuring smooth migrations, upgrades, and integrations.

With over a decade of collaboration with SailPoint as a trusted implementation partner, Avancer has empowered numerous organizations to secure their digital identities using SailPoint's IdentityIQ and Identity Security Cloud (ISC) platforms.

Over the years, we have further strengthened this relationship by proudly sponsoring SailPoint Navigate. From engaging sessions to interactive booths, our presence at Navigate underscores our commitment to advancing identity security. This collaboration reflects our dedication to helping organizations achieve seamless, secure, and scalable identity management while fostering a deeper connection with the SailPoint community.

AVANCER IN NEWS

MoneyLive – Thales x Avancer

THALES
Building a future we can all trust
elcome Identity Platform
anks & FinTech | Safeguard Digital Identities
ticate
Onboarding
THALES
OneWelcome Signature Partners
avancer

At MoneyLive, held on September 15-16, 2024, at The Radisson Blu Aqua Hotel in Chicago, we were thrilled to partner with Thales to showcase how modern identity solutions are revolutionizing the banking sector's digital landscape. Our collaborative efforts highlighted the transformative power of our joint Customer Identity and Access Management (CIAM) solutions, designed to enhance both security and customer experience in the financial industry.

Throughout the event, attendees visited us to learn about our innovative approaches to digital identity management. By combining Thales' expertise with Avancer's cutting-edge solutions, we demonstrated how organizations can better secure customer data while streamlining access processes.

12th Cyber Security Summit

On November 17, 2023, Avancer proudly sponsored the 12th Edition of the Cyber Security Summit at the Sheraton New York, Times Square Hotel. As a leading IT security solutions provider, Avancer is dedicated to empowering businesses against evolving cyber threats. Attendees had the opportunity to explore our innovative IAM products and services designed to secure critical data.

The summit featured key discussions on pressing topics such as defending against ransomware, navigating data privacy and compliance, and leveraging cloud security while addressing its vulnerabilities. Our IAM solutions were highlighted as essential tools for enhancing security, streamlining workflows, and ensuring compliance in today’s digital landscape.

AVANCER IN NEWS

Identiverse 2024

Team Avancer participated in Identiverse 2024, held from May 28-31 at the ARIA Resort and Casino in Las Vegas. This event presented an incredible opportunity for industry leaders to explore the latest advancements in IAM.

At our booth, IAM specialists engaged with attendees, showcasing innovative solutions designed to empower organizations' security strategies. Visitors gained in-depth insights into our flagship product, Identity Bridge, discovering how it can revolutionize their IAM landscape.

Identiverse also provided exceptional networking opportunities, allowing participants to connect with peers, industry experts, and thought leaders in a collaborative environment.

The event proved to be a valuable experience for all involved, enhancing IAM practices and fostering discussions around building robust and resilient security frameworks.

SailPoint SAILforward 2024

At SailPoint SAILforward 2024, held in Las Vegas, Avancer proudly participated as a trusted partner, showcasing our extensive collaboration with SailPoint on various resell and implementation projects. Our team was excited to connect with SailPoint sales professionals, build valuable relationships, and explore new avenues for mutual success.

Throughout the event, we engaged with industry leaders to discuss the latest advancements in identity governance and management. Our commitment to delivering top-notch solutions was evident in the insights shared and the discussions held.

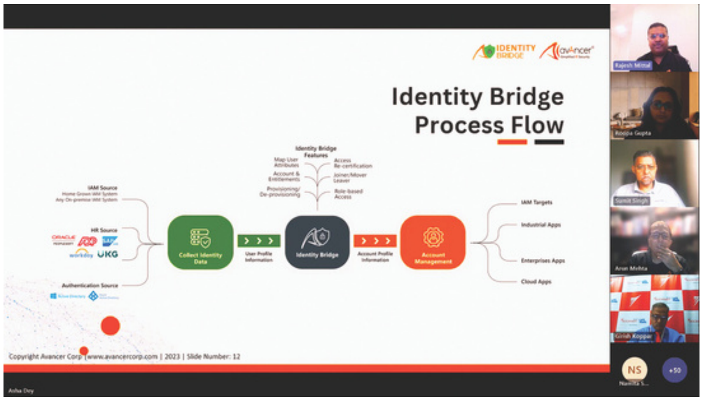
AVANCER IN NEWS

Webinar: Securing Healthcare with IAM Solutions

On December 7, 2023, Avancer Corp hosted a successful webinar titled "Securing Healthcare: IAM Solutions for Healthcare InfoSec Leaders," aimed at Security C-Suite professionals and IT Heads from leading Indian hospitals. In collaboration with Hospital Tech, the event attracted over 70 attendees and addressed critical issues surrounding Identity and Access Management (IAM) in the healthcare sector.

The webinar featured insights from IAM experts Rajesh Mittal and Arun Mehta, alongside Roopa Gupta, who discussed the challenges faced by healthcare organizations, including data sensitivity, insider threats, and compliance requirements. The presenters highlighted Avancer's IAM solution, Identity Bridge, which streamlines identity processes and enhances security by automating access control.

Key features of Identity Bridge, such as seamless integration, quick deployment, and robust access governance, were showcased, emphasizing its ability to simplify identity management and ensure compliance. Participants left with valuable knowledge on managing user lifecycles effectively, reinforcing the need for scalable and compliant IAM solutions.



Identity Bridge Process Flow

IAM Source
Home Grown IAM System
Any On-premise IAM System

HR Source

Authentication Source

Collect Identity Data

User Profile Information

Identity Bridge Features
Map User Attributes
Account & Entitlements
Provisioning/ De-provisioning
Access Re-certification
Joiner/Mover Leaver
Role-based Access

Identity Bridge

Account Profile Information

Account Management

IAM Targets
Industrial Apps
Enterprises Apps
Cloud Apps

Copyright Avancer Corp | www.avancercorp.com | 2023 | Slide Number: 12

To delve deeper into the insights shared during this impactful session, we invite you to watch the full webinar. Click here to access the recording and discover how Avancer's IAM solutions can transform security in the healthcare sector.

Avancer

Leading the future of Identity Security

- Strategic IAM Advisory Acumen
- Full Lifecycle IAM Implementation
- Rapid & Tailored App Onboarding
- Trusted IAM Management
- Certified Product Experts
- Secure Epic & Cerner Integration

Industry Specialization

- Healthcare
- Financial Services
- Manufacturing
- Retail

Talk to Our IAM Experts!

avancer
Simplified IT Security