VIEW POINT

UNLOCKING DIGITAL TRANSFORMATION

THE IMPERATIVE OF IDENTITY AND ACCESS MODERNIZATION IN CYBERSECURITY

Infosys®
Navigate your next

Abstract

In today's rapidly evolving digital landscape, businesses must adapt and innovate to remain competitive. At the core of this transformation is the need to leverage technology for efficiency, agility, and growth, making digital transformation a strategic imperative. This process involves adopting technologies such as cloud computing, data analytics, artificial intelligence, and the Internet of Things to fundamentally alter business operations, customer experiences, and organizational culture.

Identity and Access Management (IAM) has undergone a significant shift, evolving from a simple user account management tool to a Identity and Access Management (IAM) has evolved significantly, transitioning from a tool for user account management to a critical technology for digital business. Modern IAM solutions now support diverse identity types, including consumers, devices, and services, forming the backbone of seamless customer experiences in competitive digital environments.

Traditional cybersecurity measures are insufficient, necessitating a more proactive and adaptive approach. IAM is integral to this security ecosystem, enabling organizations to enhance support for their networks and improve reliability and scalability by transitioning IAM solutions to the cloud.

IAM modernization is essential for securing digital assets, encompassing strategies and technologies to improve identity governance, minimize risks, and facilitate secure collaboration. Challenges such as infrastructural and operational complexities must be addressed to advance modernization efforts, leading to enhanced security, customer engagement, operational efficiency, and agility.

This paper talks about the key pillar of IAM modernization – Zero Trust, Cloud Migration and Simplifications. We cover various approaches that an organization should consider based on their journey and what stage they are. We also try to cover the successful IAM modernization tenets which involves the right blend of people, processes, and technology.

Unlocking Digital Transformation: The Imperative of Identity and Access Modernization in Cybersecurity

In today's rapidly evolving digital landscape, businesses are constantly challenged to adapt and innovate to stay competitive. At the heart of this transformation journey lies the need to harness the power of technology to drive efficiency, agility, and growth. Central to this endeavor is the concept of digital transformation.

Digital Transformation: What is it and why is it important?

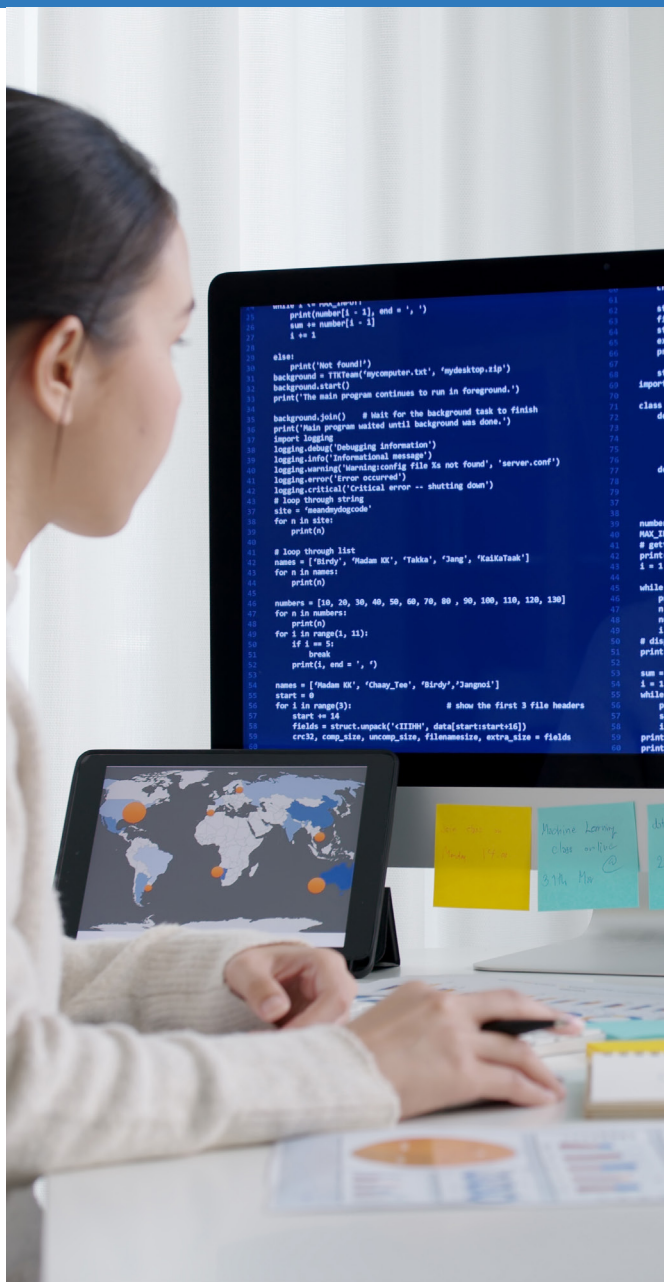
Digital transformation is more than just a buzzword; it's a strategic imperative for organizations looking to thrive in the digital age. It encompasses the adoption of digital technologies to fundamentally alter business processes, customer experiences, and organizational culture. From cloud computing and data analytics to artificial intelligence and Internet of Things (IoT), the possibilities are endless.

But why is digital transformation important? Simply put, it's about survival. In today's hyper-connected world, businesses that fail to embrace digital innovation risk obsolescence. Whether it's meeting customer expectations, staying ahead of competitors, or adapting to market shifts, digital transformation is essential for staying relevant and resilient in an increasingly digital-first economy.

Contemporary digital enterprises require a robust and comprehensive IAM solution that encompasses diverse identity types.

IAM has transformed significantly over the past two decades, evolving from a mere administrative tool for user account management to a pivotal technology driving the Digital Business forward. Its evolution has shifted from a primary focus on managing workforce identities to encompassing all identity types, including consumers, devices, objects, and services.

A modern IAM platform serves as the cornerstone for crafting seamless customer experiences, which are paramount for digital organizations seeking to excel in today's competitive landscape.



Strengthening the Cybersecurity Posture

As organizations embrace digital transformation, they must also grapple with the escalating threat landscape. Cyberattacks are becoming more sophisticated and frequent, targeting sensitive data, disrupting operations, and eroding trust. In this context, cybersecurity emerges as a critical priority for safeguarding assets, mitigating risks, and preserving brand reputation.

However, traditional cybersecurity approaches are no longer sufficient in today's dynamic threat landscape. A more proactive and adaptive approach is needed.

IAM plays a vital role within the security ecosystem, serving as a crucial component. As organizations strive to enhance the support for their customer and employee networks while improving reliability and scalability, they are increasingly transitioning their IAM solutions to the cloud as part of their modernization efforts.

Modernizing Identity and Access Management: An Essential Foundation of Cybersecurity

IAM modernization represents a paradigm shift in how organizations manage and secure access to their digital assets. It encompasses a range of strategies and technologies aimed at enhancing identity governance, minimizing risk exposure, and enabling secure collaboration across diverse environments.

Challenges such as infrastructural and operational complexities, including inadequate integration among applications and cloud solutions, outdated technology, and organizational silos, can hinder the journey toward modernization. However, by streamlining and consolidating these elements within their IAM strategy, organizations can effectively advance their modernization efforts. Consequently, they can achieve comprehensive enhancements in various business facets such as security, customer engagement, operational efficiency, and agility.

Key Pillars of IAM Modernization

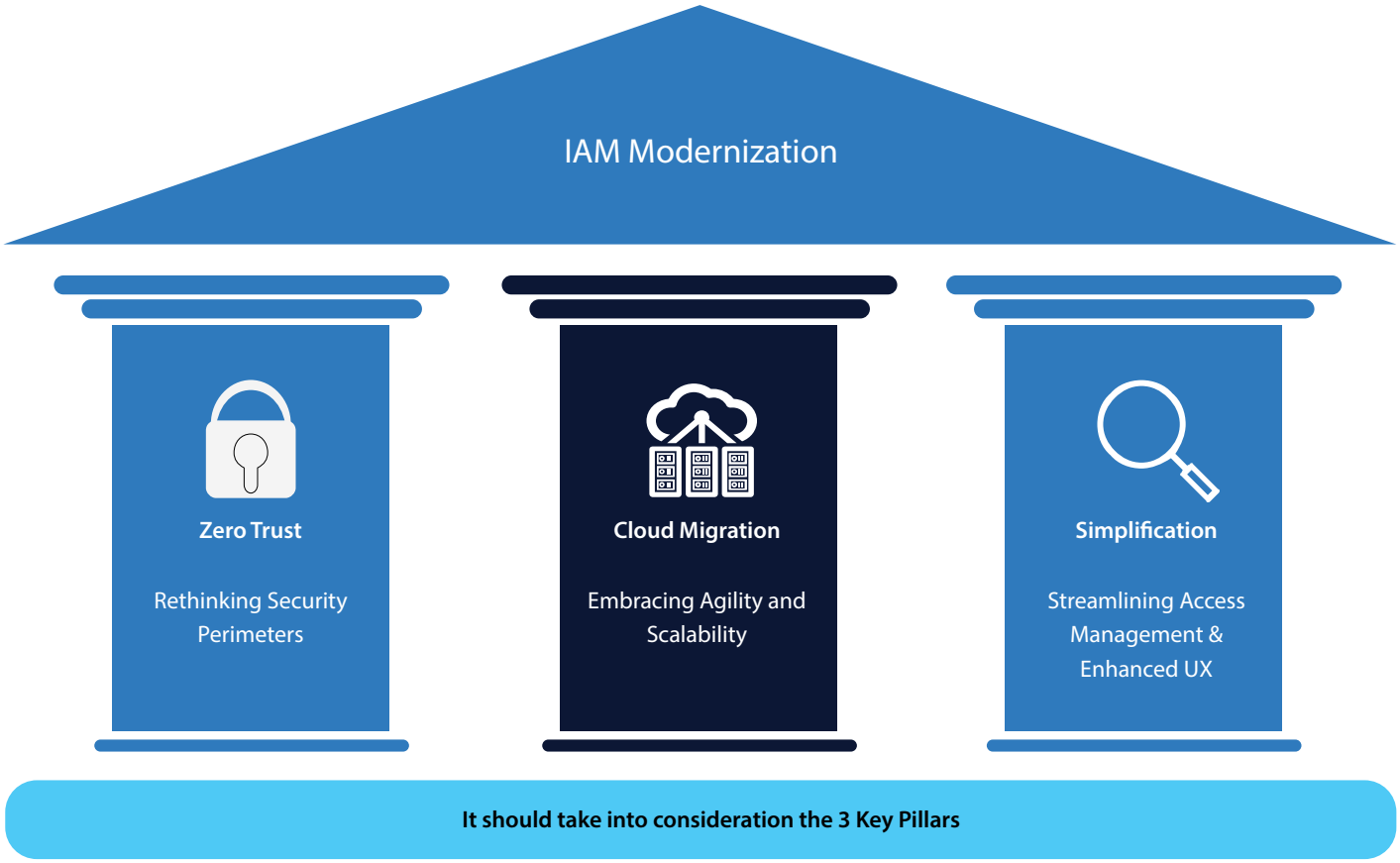


Figure 1 : Key Pillars of IAM Modernization

A. Zero Trust: Rethinking Security Perimeters

Traditional security models operate on the assumption of trust within the network perimeter—a notion that is increasingly untenable in today's decentralized and perimeter-less environments. Zero Trust challenges this paradigm by adopting a "never trust, always verify" approach to security. It verifies identity and authorizes access based on multiple factors, such as user context, device posture, and behavioral analytics, regardless of whether the user is inside or outside the corporate network. By implementing Zero Trust principles, organizations can reduce the risk of unauthorized access and lateral movement within their digital ecosystems.

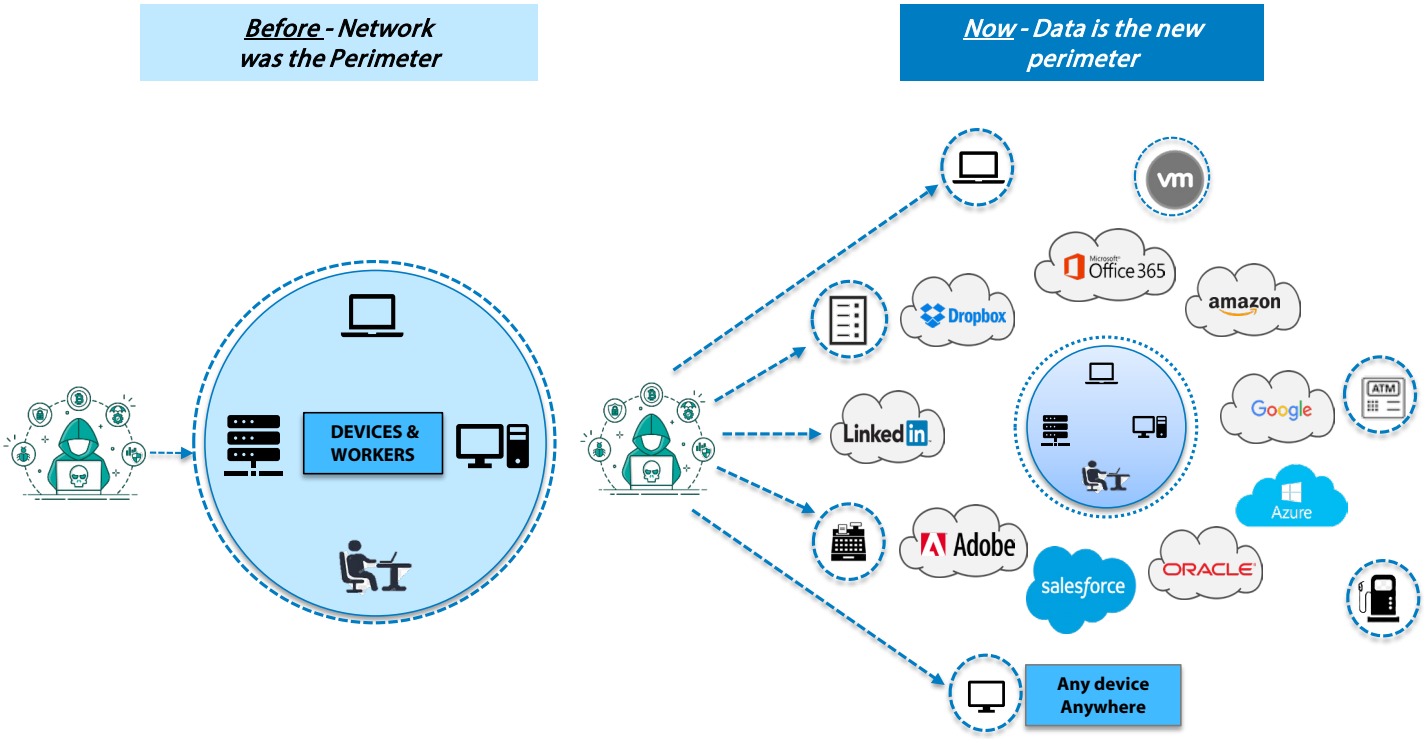


Figure 2 : The new reality - Blurring boundaries leading to exponential rise in Security breaches

Identity serves as the cornerstone of the Zero Trust approach[2], a security paradigm that prioritizes continuous verification over blind trust in individual systems. The mantra of "Don't trust, always verify" forms the bedrock of Zero Trust principles, which have expanded beyond Zero Trust Network Access[3] (ZTNA) to encompass identities, devices, networks, systems, applications, data, and software.

At the heart of Zero Trust lies identity and authentication, emphasizing the importance of knowing who is accessing the system and from which device. Integration of IAM with endpoint detection and response (EDR), including endpoint management, becomes indispensable in this context. Users undergo authentication and authorization at the endpoints and networks they interact with, ensuring secure access to systems, applications, and data.

IAM assumes a pivotal role in Zero Trust by controlling both authentication and access permissions, thus initiating and concluding the verification process. Technologies like adaptive authentication, which factor in risk and context, alongside access management for systems, applications, and data, play a central role in Zero Trust implementations. Indeed, Zero Trust is inseparable from IAM.

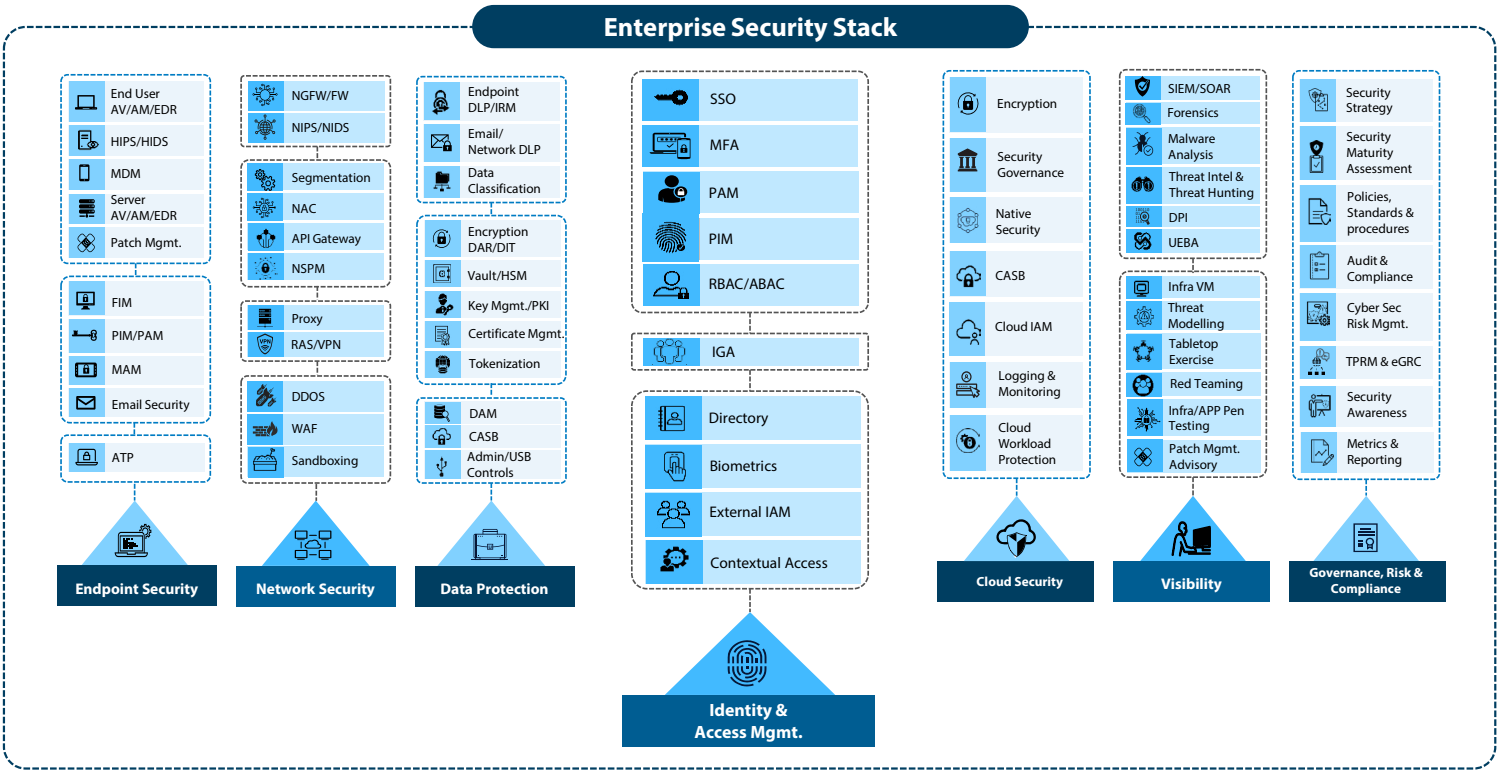
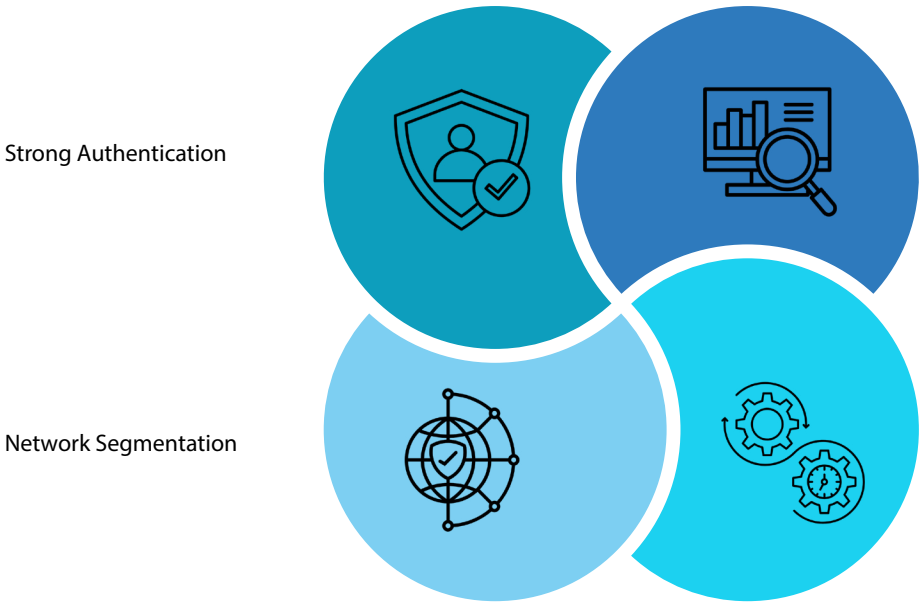


Figure 3 : Applying Zero Trust Security to Enterprise IT fabric with comprehensive controls and tools

While legacy IAM solutions offer single sign-on access for all applications, modern IAM solutions employ access evaluation on a per-app, per-policy, and per-login attempt basis, ensuring that Zero Trust principles are ingrained throughout the system.

Hence to achieve the goal of ZTNA (Zero Trust Network Access), we need to keep below key points:



a) Cloud Migration: Embracing Agility and Scalability

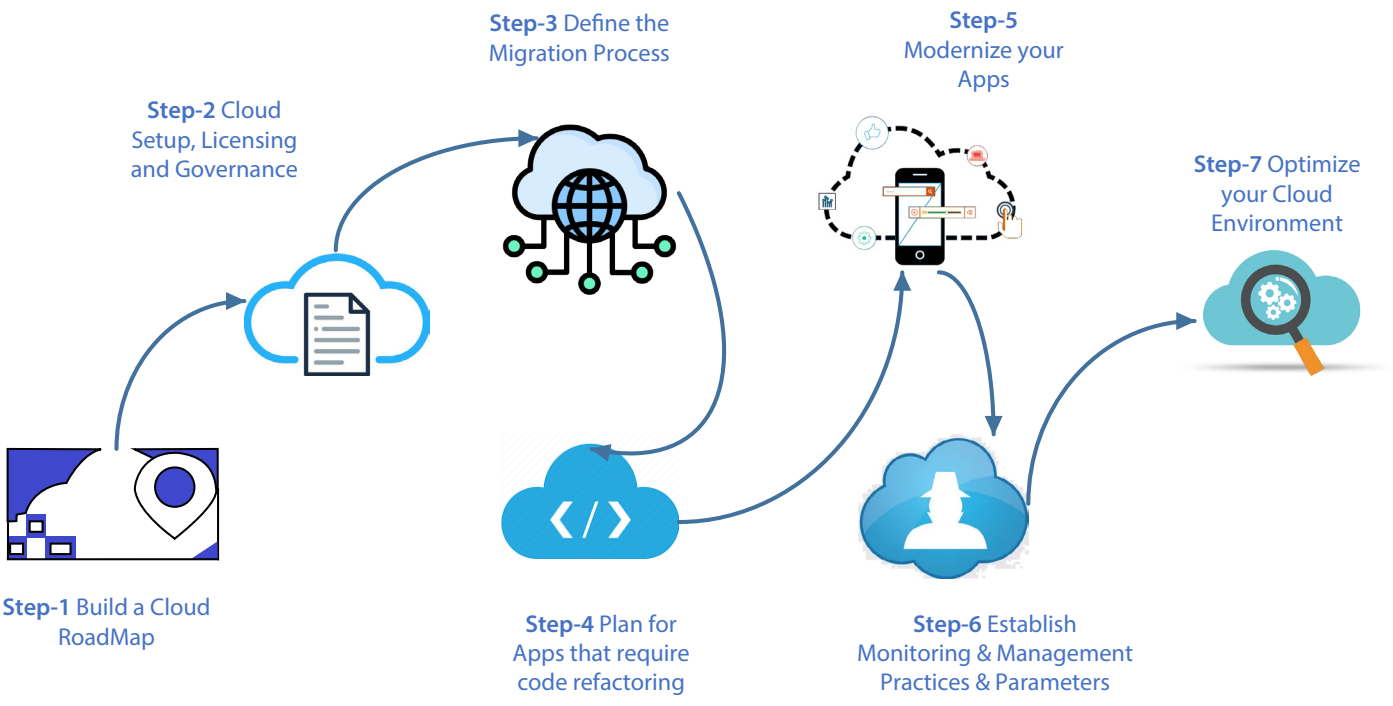
The migration to cloud-based environments is a cornerstone of digital transformation, offering unparalleled agility, scalability, and cost efficiencies. However, this shift also introduces new security challenges, particularly around Identity and access management. IAM solutions tailored for the cloud era provide centralized visibility and control over user access, data, and applications across multi-cloud and hybrid environments. By integrating IAM seamlessly into their cloud migration strategies, organizations can ensure that security remains a top priority without compromising on the benefits of cloud adoption.

As cloud-based applications and distributed computing models become the increasingly prevalent, traditional solutions are no longer sufficient to address the requirements of contemporary IAM. Migrating to cloud is the first step in modernizing the IAM Landscape. By completing the migration, the enterprise is laying the foundation for a more modern, agile, and secure IAM solution.

According to a report by Forrester, decision-makers in the realm of IAM unanimously recognize the importance of fully transitioning their identity security technologies to the cloud as a crucial element for success. This significance is particularly accentuated for organizations employing both CIAM and workforce/employee IAM solutions, with 92% of them emphasizing the critical nature of migration. This underscores the amplified and positive impact of cloud migration, especially for organizations leveraging multiple IAM technologies.

Despite this acknowledgment, progress in migration efforts among IAM decision-makers has been sluggish. Forrester's findings reveal that only 12% of security decision-makers have completed the full migration of their IAM solutions to the Cloud[1]. Presently, modern IAM solutions predominantly adopt a hybrid approach, with surveyed organizations hosting 37% of their security technologies in traditional on-premises environments. However, there's an anticipated shift in the coming two years, with this figure expected to decrease by 7% (reaching 30%) as more organizations opt to migrate a larger portion of their security infrastructure to private cloud (40%) and public cloud (30%).

To embrace such a strategy, we need to have a clear roadmap as below:



There are multiple approaches for cloud migration[4], an organization should decide the best suited one for them depending on the industry standards, timelines, resource gathering and costs.

a) Lift and Shift

The Lift and Shift approach involves transferring the existing production environment from on-premises data centers to cloud-based technologies with minimal modifications.

Migration Process Steps:

Note: Ensure necessary ports and URLs are transferred and opened.

1. Take the latest backup from the backup team and migrate the data to newly created servers (App or Web) on the cloud with similar configurations.
2. Migrate the database using RMAN or Dump file procedures from on-premises data centers to cloud servers, maintaining similar configurations.
3. Start services and perform thorough testing and monitoring.
4. Configure initial connectivity between on-premises data centers and the cloud for data replication of accounts.

Pros:

1. Quick migration from data centers to cloud-based platforms.
2. No need for team retraining, as the process is similar to that of data centers.
3. Reduces time constraints during tight deadlines.

Cons:

1. High dependency on multiple teams for the migration process.
2. Limited control over the cloud environment.
3. Does not fully leverage the potential of cloud technologies.
4. Costs remain similar to data centers, as charges apply per cloud interaction.

b) SaaS Cloud

The SaaS Cloud approach enhances user efficiency and minimizes errors through improved usability and configuration options.

Key Benefits:

- Improved usability that consolidates information on logical panels.
- Additional configurability options, extension points, and enhanced backup operations.

Migration Process Steps:

1. Install the database and IAM using cloud frameworks and federations.
2. Segment services for applications, web, and databases, utilizing full cloud control.
3. Move data using the IAM export utility for applications, web, and RMAN for databases.
4. Ensure services are located within similar zones and VPCs.

Pros:

1. Full utilization of cloud-based infrastructure.
2. Adopts a true SaaS approach.
3. Services can be easily configured to start and stop on the cloud.
4. Capability to integrate generic AI solutions.
5. Eliminates the need for repeated port openings.
6. Simplified deployment features.
7. Lower costs due to efficient use of cloud features.

Cons:

1. The team must have a basic understanding of cloud usage and frameworks.
2. Integration from on-premises data centers to the cloud requires time for initial setup.
3. Limited choices concerning available products.

c) Containerization

Containerization involves setting up environments similar to virtual machines but with a smaller footprint due to their relaxed isolation properties. They use a stateless and immutable setup to isolate the IAM solution from other applications.

Key Features:

1. Dedicated CPU shares
2. Dedicated filesystems
3. Dedicated process spaces and memory
4. Capability to use the OS among other applications due to their lightweight, relaxed properties

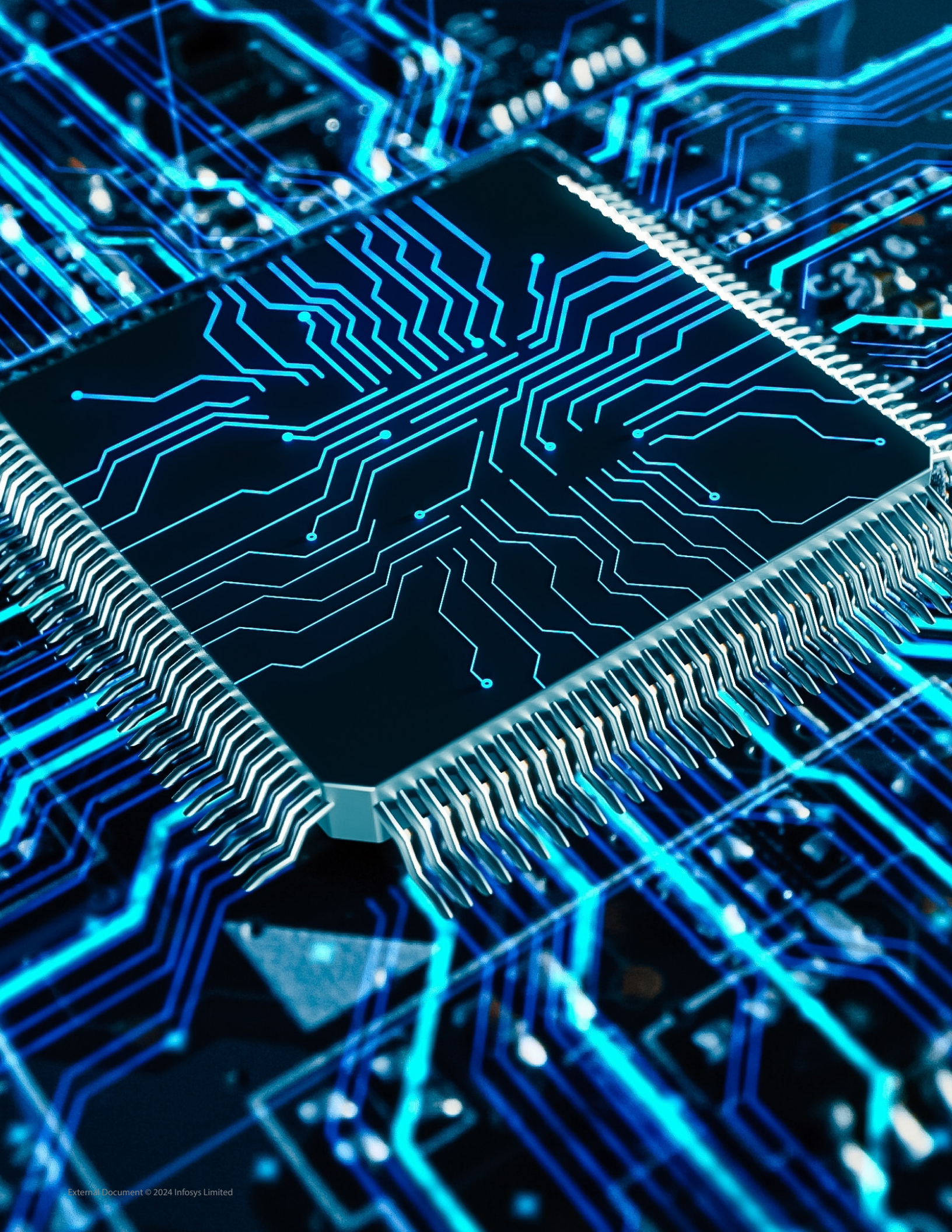
The setup process is similar to the Lift and Shift approach from on-premises data centers to containers, but it eliminates the need for ongoing port openings once the initial setup is defined.

Pros:

1. Applications remain isolated from shared services.
2. Applications are not affected by server patching.
3. Applications are insulated from downtimes.

Cons:

1. The team needs to understand container technology.
2. The team needs to know how to build manifests for their applications.



b) Simplification: Streamlining Access Management & Enhanced Experience

Complexity is the enemy of security. As digital ecosystems grow increasingly complex, managing identities and access rights across disparate systems and applications becomes a daunting task. IAM modernization seeks to simplify this complexity by consolidating identity silos, standardizing access policies, and automating routine administrative tasks. By streamlining access management processes, organizations can enhance security, improve operational efficiency, and reduce the risk of human error.

As organizations embark on IAM modernization initiatives, the adoption of a straightforward identity management solution emerges as a critical priority. While custom-built or in-house identity solutions may appear attractive, they often entail significant resource investment and ongoing maintenance efforts.

Conversely, off-the-shelf identity management platforms may lack the specialized insights necessary to effectively address the nuanced challenges specific to particular industries.

Opting for modern, cloud-based solutions tailored to the intricacies of specific industries enables organizations to seamlessly integrate a diverse array of legacy, contemporary, and cloud-based applications.

Simplicity is key, with the overarching goal of enhancing both internal and external user experiences. IAM modernization endeavors should prioritize improved customer experiences, particularly for customer-facing applications, as a primary outcome.

Things to consider when you are ready for IAM Modernization Journey - People, Process & Technology

Once the right technology and approach is finalized below should be considered from People and Process perspective:

People

Right Resources which include Project Manager, Technical Subject Matter Experts (SMEs), Test Manager, Business Analyst, Database Administrator, Cloud Governance, Enterprise Architect, Cloud Architect, Enterprise Cybersecurity team, Unix and Windows Admins.

Process

Establishment of cloud (Migration of AC-DC), Technical Documentation (Step by Step activities), DR-Site, Project Plan, Execution Plan, Test Plan and Rollback Plan, Port openings planning, Communication Plan, Planned Downtime for cut over, Infant care period, Detailed ETS.

Also, proper Co-ordination and communication is very important between core team, Vendor SMEs and other supporting teams. A detailed RACI should also be created and socialized.

Summary

In today's dynamic digital era, businesses must undergo digital transformation to stay competitive and relevant. Central to this transformation is the modernization of Identity and Access Management (IAM), which has evolved to include a wide range of identities, such as consumers and devices, beyond traditional workforce management. Modern IAM solutions are vital for delivering seamless customer experiences, bolstering cybersecurity, and improving operational efficiency. Key strategies for IAM modernization include adopting Zero Trust principles, transitioning IAM solutions to the cloud for enhanced agility and scalability, and simplifying identity management processes to reduce complexity and risk. Addressing challenges such as infrastructure integration and operational silos is crucial for a successful modernization journey. By focusing on the right combination of people, processes, and technology, organizations can achieve enhanced security, agility, and growth, ensuring they thrive in an increasingly digital-first economy.

About the Authors

Sal Fazal

Sal Fazel works as a Product Manager for Identity and Access Management (IAM) Team in Cummins Inc. He's responsible for the IAM Team, platforms, product portfolio, and adherence to Global Cybersecurity processes, policies and procedures. Sal has over twenty years of experience in the field of IT/Cyber. He has taught courses at Indiana University's Department of Informatics.

Aditya Gupta

Results-driven cybersecurity leader and enthusiast with a successful record of implementing robust cybersecurity strategies to manage risks and safeguard organizational assets. Working as Principal Consultant with Infosys with over 21 years of experience developing, implementing, and leading global transformations & cyber security programs across diverse cyber domains. An MBA and Engineer by education, he also holds various Industry certifications like CISSP, CCSP, CCNA & OCI Security Professional.

References

1. Only 12% of security decision-makers have completed the full migration of their IAM solutions to the cloud, Forrester Opportunity Snapshot: A Custom Study Commissioned by PING IDENTITY and FORGEROCK, NOV 2023
2. Zero Trust: Rethinking Security Perimeters, Infosys Knowledge Institute, 2024
3. To achieve the goal of ZTNA (Zero Trust Network Access), we need to consider Strong Authentication, Network Segmentation, Monitoring and Regularity in Updates and Vulnerability Scans, Forrester The Business Of Zero Trust Security, 2024
4. Steps for Cloud Migration, Infosys Cybersecurity IAM Center of Excellence, 2024
5. Importance of IAM Modernization, NIST Identity and Access Management Roadmap: Principles, Objectives, and Activities, April 21, 2023

For more information, contact askus@infosys.com

Infosys®
Navigate your next