AVANCER CORP

FUTURE OF IDENTITY AND ACCESS GOVERNANCE CAPABILITIES AMIDST TECHNOLOGY DISRUPTION

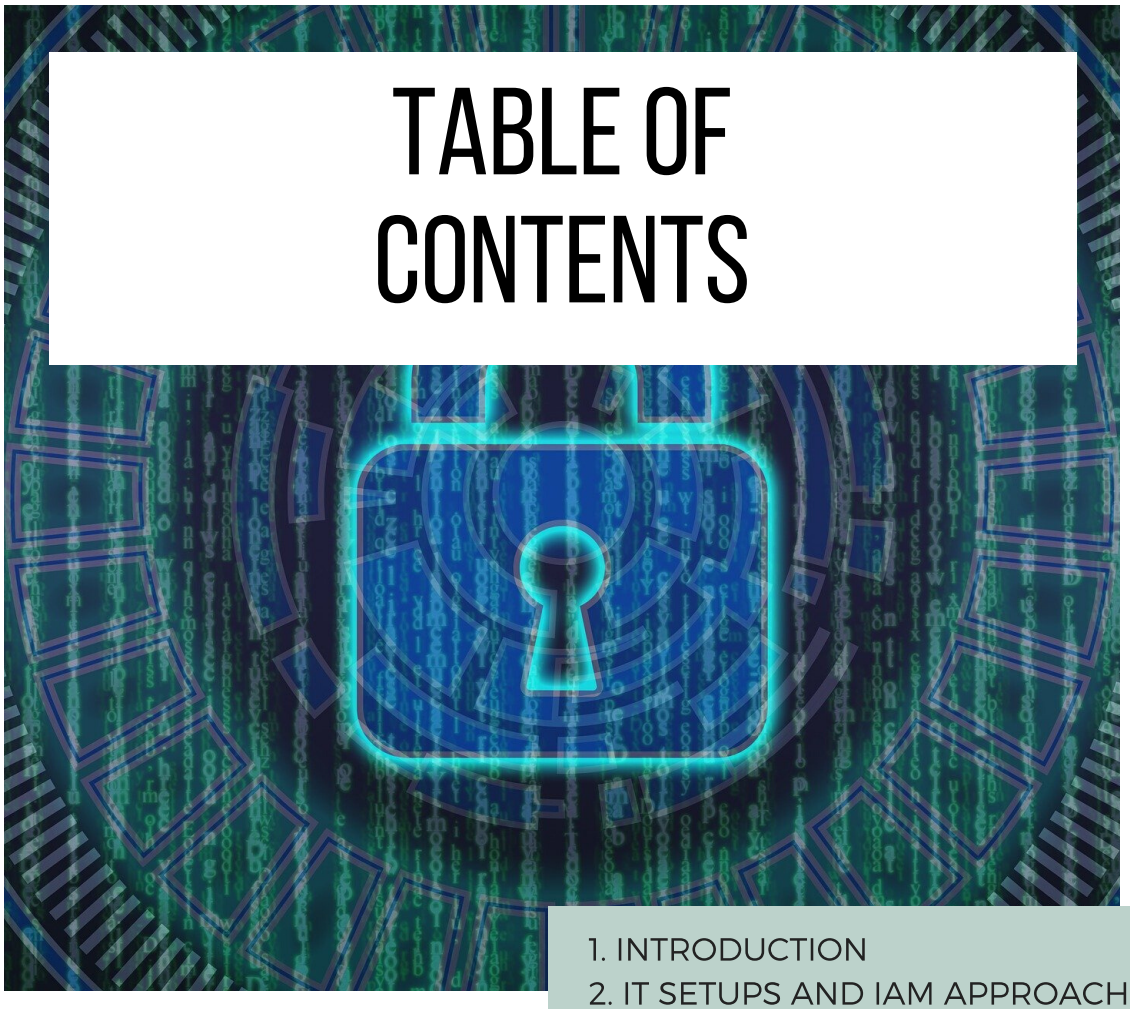
EVOLUTION OF IAM WITH GROWING TECHNOLOGICAL INNOVATION

FEB 2020

The e-book focuses on how identity and access management is expected to evolve in the near future amidst the explosion of disruptive technologies.

FEBRUARY 2020

TABLE OF CONTENTS



1. INTRODUCTION
2. IT SETUPS AND IAM APPROACH
    2.1. DEPLOYING IAM ON-PREMISE
    2.2. DEPLOYING IAM IN THE CLOUD
    2.3. DEPLOYING A HYBRID IAM PLATFORM
3. THE NEED OF THE HOUR
    3.1. CREATING A HOLISTIC IDENTITY SOLUTION
    3.2. EVOLUTION OF IAM SYSTEMS
4. WHAT'S IN STORE FOR FUTURE? FUTURISTIC IAM INNOVATION
AVANCER'S EXPERTISE IN IAM

1. INTRODUCTION

BIG DATA ANALYTICS, MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE (AI) ARE BEING INTEGRATED TO IMPROVE PROCESSES AND USER EXPERIENCES

Enterprises globally are investing in digital transformation using disruptive technologies leading to gradual suspension of legacy systems usage. Advancements such as Internet of Things (IoT), Big Data analytics, machine learning (ML) and artificial intelligence (AI) are being integrated to improve processes and user experiences in almost all verticals of businesses. As per a report by Genesys, provider of omnichannel customer experience and contact center solutions by 2020, 60 per cent of US-based companies would be using AI to improve staffing, operations, budgeting and performance[i].

However, with the emergence of newer technologies, there are vulnerabilities in the IT ecosystem especially with managing digital identities.

A strong risk management strategy is required to prevent any breaches due to internal or external threat which may result into reputation and revenue loss.

Digital identities are core to the usage of any technology – thereby, making regulatory bodies and industry standards organizations, globally, concerned about the impact of digital identities on privacy rights of users. With the advent of stringent data privacy regulations, such as the European Union General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA), the challenge is to protect the privacy of users without compromising user experience and business goals.

To protect the privacy of the users, enterprises need to ensure that users are provided with the right access to the right resources at the required moment for a verified reason.

In the current dynamic technological world, a user often has several identities created on different platforms, apps and devices. To add to the complexity, the infrastructure hosting these systems could be deployed on premise, cloud based or a hybrid model.

However, creating a secure ecosystem is often seen to be developed at the cost of usability, which has become a huge barrier in the adaption of IAM technologies such as multi-factor authentication (MFA). Thus, a holistic approach to managing digital identities in the face of technological innovation is the need of the hour – creating an IAM system that provides seamless user experience while securing the businesses, along with complying with policies and regulations.

IAM challenges in changing digital landscape

Many organizations have identities stored in various locations within the network infrastructure.

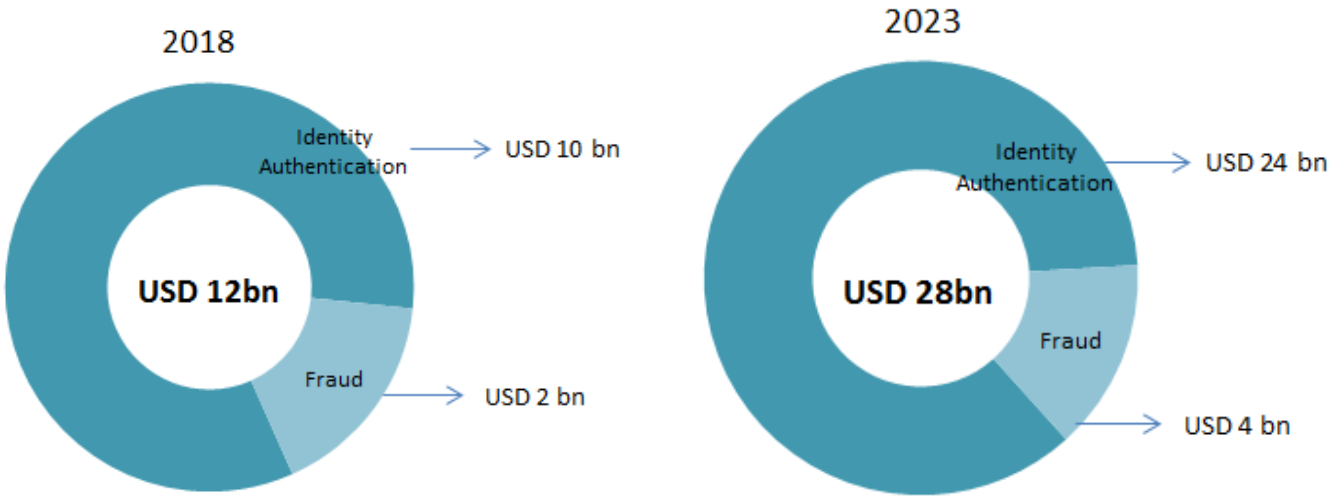
Digital identities can no longer be managed in the usual ways, thereby, requiring enterprises to evolve identity and access management (IAM) strategies that are not only consistent with the growing need and scope of modern identity environments but also evolve as per the future requirements in identity solutions.

In fact, the identity authentication and fraud solutions market is expected to reach USD 28 billion in 2023 from USD 12 billion in 2018, as per BCG[ii].

This makes managing identities and creating a proper approval process for access provisioning difficult for both security professionals and users requesting access. Any roadblocks faced by users while requesting access results in escalations, often times, to the management and overriding the approval process. With this, professionals given the responsibility of approving requests have little or no knowledge about whether or not to give access to employees to confidential data.

Yet another challenge that the organization faces is lack of authoritative and centralized repository for users. This furthermore makes the process of identity reconciliation a substantial challenge. The basis to create identity reconciliation is not just

The market for Identity Authentication and Fraud Solutions will reach USD 28 billion by 2023



Source: BCG Research and Analysis

to provision access rights that have been granted or requested for, but it also needs to import actual accounts and focus on access rights that are from connected systems.

Furthermore, with regards to accreditation and certification, auditors may not have adequate knowledge about access requirements, which they might be required to provide to multiple users. This often leads to resorting to manual provisioning, which could be cumbersome and inconsistent, resulting in higher risk of the system being non-compliant or creating duplicate and redundant identities. Some of the other issues include lack of support in case of centralized access management solutions. These include directories as well as single sign-on (SSO), non-existent or outdated access management policies or failure to establish rule-based access, such as removing identities and access privileges automatically with the termination of an employee. Time-consuming and strenuous audits might only make the process far more tiresome.

Evolution of IAM as per business requirement

Organizations are adopting mobile technology that enables bring-your-own-device (BYOD) policies. This helps employees in accessing corporate data from remote location as well. IAM is able to provide foundational security component across the enterprise which connects to mobile platforms irrespective of user's location.

Cloud services are also adding to complexity to the IAM equation. This is forcing organizations for operating their capabilities on-premises as well as integrating similar capabilities offered by the cloud service provider (CSP). In such a situation, hybrid identity management solution could be a way forward, wherein, a single user identity could be created for authentication and authorization to all resources irrespective of their location, whether in on-premise or on-cloud. Federated access – the role-based access as well as cloud-based IAM solutions – may help in addressing these requirements.

Identity-as-a-service or IDaaS could be another effective solution which may help accelerate IAM deployments in the cloud environment. IDaaS is able to support federated authentication, provisioning and authorization. It is also considered as a viable alternative to on-premises IAM solutions. In terms of return on security investment, IDaaS is able to remove the cost of implementing on-premises solution.

It might be vital to understand the need for IAM capabilities that effectively govern access for hosting app internally. In case of hybrid cloud IAM model, IDaaS solution would need APIs or appliances that are able to operate within the IT infrastructure for completely outsourcing the function. Most enterprises face risks in securing these agents and interfaces, which needs to be managed.

Data loss prevention through IAM

Security professionals often provide information about an identity retrieved from an IAM system to DLP – Data loss prevention – solution, which focuses on monitoring sensitive data and correlating trends / events for reducing risk of data loss. These events could be correlated with analytical artificial intelligence along with machine learning tools. These tools are able to analyze historical behavior for detecting potential fraud.

IAM as well as DLP solutions could be leveraged for addressing insider threats together with emerging threat vectors. Additional monitoring capabilities could be provided by incident forensics tools and behavioral analytics.

With the integration of these solutions, organizations could handle the changing IT trends and the threats posed by mobile and cloud computing.

Securing social media identities

Given the current scenario, organizations are able to leverage social media for interacting with customers. They are looking at increasing brand awareness as well as creating a repository of common identity. However, if these social identities are breached, companies might face legal, operational, regulatory and reputational risks – thereby negatively impacting their customer base.

Strong IAM solutions, including MFA, should be deployed by social media services for protecting the corporate accounts. Additionally, cyber analysts should get alerts for users with failed login attempts, especially from different geographical locations. Creating security awareness and educating your employees about social media security should be a regular exercise.

IAM AS WELL AS DLP SOLUTIONS COULD BE LEVERAGED FOR ADDRESSING INSIDER THREATS TOGETHER WITH EMERGING THREAT VECTORS.

2.IT SETUPS AND IAM APPROACH

A pertinent question related to leveraging IAM amidst technological advancement is selecting the most efficient deployment model – whether to choose on-premises, cloud-based model or hybrid setup. Selection of an IAM solution and its implementation method will depend on an organization's security profile and applicable regulations. However, every approach comes with its own challenges. Let's have a look at some of the challenges and possible solutions to deploy IAM on various IT setups:

2.1 Deploying IAM On-Premise

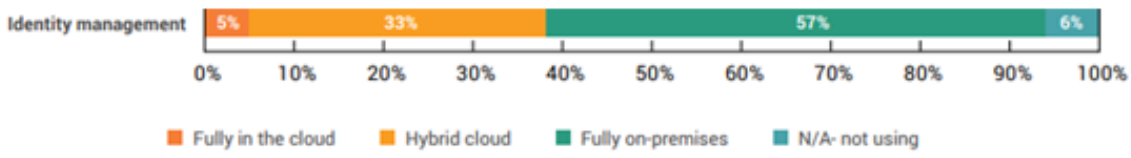
While cloud computing technology is seen to be disrupting the way businesses are operating in the current IT ecosystem, many enterprises are still running their services and applications on-premises.

Often concerns related to latency, privacy, security or regulations compel organizations to depend on legacy systems. In fact, according to a survey by Spiceworks[1ii] of more than 450 IT decision makers across North America and Europe, "59% of businesses run their database servers fully on-prem, while 57% run their identify management systems and 46% run their ERP software on-prem as well[iv]."

The on-premise deployment model is able to provide complete control of your data and helps in managing security. Given this opportunity, it provides a valid option for any organization which has dedicated staff, money, time as well as technical expertise for managing such solutions.

However, the on-premises model requires IAM solutions that have significant infrastructure along with platform footprint.

It might become very cumbersome for providing continuous resource availability or support when migrating from one vendor to another. Further, there might be problems with upgrades – which may not make it into the priority list.



Source: Spiceworks Research

With that, on-premises may also require large, specialized staff for running and monitoring the IAM stack.

Previously, most of the business applications were situated "inside" the firewall of an organization. This allowed them to remain in a contained environment. Since, companies have started using multiple software-as-a-service (SaaS) offerings through public clouds – thus exposing their data to web-facing applications – it has put added pressure on the security environment, together with posing threat to the authentication solution. Given an on-premise solution, hardware sizing, management and capacity planning with database administration remains the focus area.

One of the best ways of addressing on-premises challenges is to invest time and discipline for assessing an organization's requirements. It is also necessary for creating thoughtful and comprehensive approach from ground up by considering all the stakeholders that might help in future integrations. This mostly includes data center capacity planning with thorough understanding of performance concerns of the business. Organization might also consider implementing private cloud infrastructure-as-a-service (IaaS) as well as platform-as-a-service (PaaS) offerings. This allows organization to get a hybrid approach, while keeping control of assets fully owned in-house.

2.2 Deploying IAM in the cloud

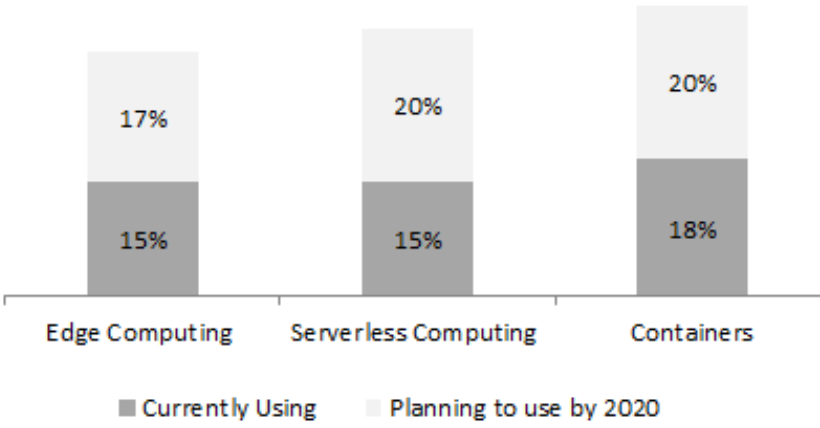
As per the survey – Public Cloud Trends in 2019 and Beyond – by Spiceworks, "69% of IT decision makers believe cloud services can enable their organization to more easily adopt emerging technologies.[v]"
In fact, as per the research the top-most cloud-based technologies that are increasingly being adapted by enterprises include serverless computing, edge computing and container technology.

On the basis of this background, it could be safe to expect that with increasing adoption of cloud computing, cloud-based IAM technology will also witness an upsurge.

While cloud-based IAM is one of the most seamless and secure model, there could be a few challenges that need to be addressed for making the system efficient and effective.

One of the challenges with this model is ensuring that access control, logging, as well as monitoring controls are designed and implemented securely. The on-premise control objectives should be made achievable in cloud too. Other challenges include shortage of experienced security experts conversant in cloud system.

Adoption of emerging cloud trend



Source: Spiceworks Research

In a cloud model, it is imperative to understand the way data has been stored – along with where and why. This becomes the most important aspect for addressing IAM cloud challenges. It is also mandatory to have a coherent cloud strategy which is able to line up with the current IAM needs, human resource needs, budget, workforce constraints and IAM architecture.

A dependable identity-as-a-service – IdaaS – platform is able to address the challenges that are associated with cloud systems. Through incorporating a different platform service in the environment, it is able to take work off

the team's plate by managing capacity planning, developing core features, and hardware, to name a few things. It is able to give time for the organization to think about implementation as well as end-user experience.

Going forward, given the explosion of technologies, organizations should also be able to measure the results alongside the expectations and accept changes in directions based on the metrics. IAM cloud strategy should be able to support IAM objectives and work within the constraints of the culture of an organization.

2.2 Deploying a hybrid IAM platform

Adoption of hybrid IT model by enterprises is usually synonymous with their digital transformation goals. It becomes less expensive and requires fewer resources as compared to implementing a full private cloud option. Hybrid deployment has been able to help organizations bridge the gap between on-premises and cloud paradigms. It is able to provide scalability and features just like a cloud environment, while maintaining the on-premises footprint that many security departments are most content with.

In fact, "41% of organizations reported running productivity apps using a hybrid cloud approach, where some workloads run locally and some are handled in a public cloud[vi]," as per the survey by Spiceworks. Further, the research states that 46 per cent organizations[vii] are seen to use hybrid model as a backup strategy, storing information both on cloud and on-premises to create redundancy, in case of disaster recovery.

However, the management overhead together with complexities in technology is higher in such cases. Thoughtful design and a complete understanding of goals for choosing such a hybrid model is the vital component for making it a success.

The best way to start such a deployment is by understanding where these tools and interfaces belong in every zone. Thereafter, ensuring the operational processes along with playbooks helps in working around with increased complexity. Maintaining high accuracy while deploying the environment is critical for successfully launching it for any organization.

In case of the hybrid model, it is very difficult to justify expenses as there are many subscriptions that have to be maintained. Further, complexity could be added when determining levels of use of private versus public cloud services. With this, as seen in the cloud model, hybrid environment can witness an increased security risk if not executed properly.

Enterprises might look at creating a hybrid platform for meeting their IAM needs. Using individual components for its strengths together with blending on-premise and cloud solutions could provide flexibility and scalability. Automation can help improve operational efficiency and reduce administrative cost. In the end, IAM solutions should be able to adapt to an enterprise's culture for being effective and aligning them as per the business goals for arriving at the results that an organization desires.

ADOPTION OF HYBRID IT MODEL BY ENTERPRISES IS USUALLY SYNONYMOUS WITH THEIR DIGITAL TRANSFORMATION GOALS.

3. THE NEED OF THE HOUR

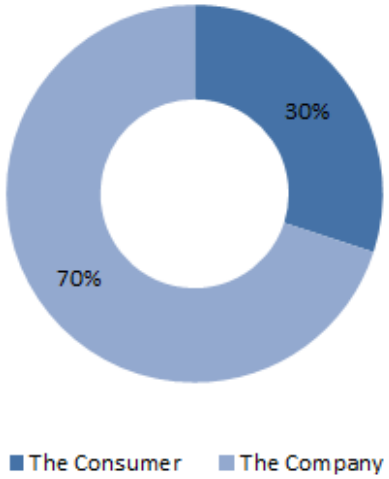
Despite identity solutions being an integral part of a holistic digital experience, users rarely want to be accountable for securing their accounts. While enterprises integrate several access management tools to secure their systems, they depend on users to follow-through the access process, which may include creating cumbersome passwords or entering verification codes from other accounts or devices. Let's look at how IAM technology could provide seamless digital access and evolve over a period of time.

3.1 Creating a holistic identity solution

Experts believe that despite interest and investments in IAM technology, the market is still adapting to keep up with the technological advancements. As per an article by BCG[viii], Some of the major challenges that are curbing expansion in the sector include:

Last-mile security adherence burden on end-users. Users find verifying and securing their identity, whether through repeated requests to change password, multi-factor authentication, or answering security queries, a burdensome task. As per a survey by Gemalto – Data Breaches & Customer Loyalty 2018 – more than 55 per cent respondents stated that they used the same password across multiple online accounts[ix]. Usage of same passwords across accounts is leaving consumer data vulnerable to breaches. Furthermore, consumers are seen to be reluctant to use added security layers such as two-factor authentication. Gemalto survey found that 39 per cent consumers did not want to use two-factor authentication to secure their social media accounts, when provided with the option.

The consumers, are therefore, relying on businesses to secure their data, rather than taking the onus to adhere to additional security measures at their end. In fact, 70 per cent respondents believe that data protection is the responsibility of the company that is storing the information. It is also worrisome to note that around 66 per cent consumers stated that they would not continue with the organization in case of any data breach[x]. Thereby, security solutions that rely on end-users adherence are not gaining significant traction, as consumers are looking for more seamless user experience.



Analysis of the average percentage of responsibility for protecting and securing customer data that respondents feel falls on the company and the customer.

Source: Gemalto survey

Identifying data is used by providers in a suboptimal manner. To ascertain the identity of a person offline, authorities and others ask for providing documents and information such as driver's licenses, social security, passports or even tax ID numbers. Further, with technological evolution, new data types have become valuable for identifying an individual's identity. These include biometrics – such as fingerprint patterns, retina scans and others. Some of the other metrics include IP addresses, geolocation data, device IDs, as well as behavioral analytics such as a user's typing style. Critically, such data types help in facilitating frictionless and automated authentication process that users often prefer, as the consumers are not required to put significant amount of efforts in establishing their identity. However, in such cases, verification is not as seamless as it should be. One of the main problems is that this data might be available with just a few sources, which are often not being accessed and integrated by identity solutions providers into their platforms.

Lack of high-end technology by the providers. Providers in most cases are not able to use the technology available to them or may not be able to use it effectively. Machine learning and artificial intelligence might be able to automate and simplify identity authentication, along with improving security and accuracy. However, these technologies cannot function in a silo. Training needs to be done for algorithms and it also requires scale. With more number of users on the platform, there would be more data points to work with, which would ensure generating effective solution. However, there has been a lot of inconsistency in the identity authentication sector. Often, IAM solutions that have promising technology might not have sufficient scale, while established players with necessary scale might not have the required technology that is innovative. In either case, identity authentication might not be utilized to its full potential.

Some of the above mentioned challenges are not able to provide full potential to identity solutions. Thus, the need of the hour is to create a holistic identity solution. If a provider is able to understand the pain points and navigate around them, it would be able to create a solution that works for all the stakeholders. Such a solution needs to be seamless for consumers, effective for enterprises and governments, while being differentiator for the provider.

For creating such a seamless, differentiating and efficient experience – solution providers including start-ups as well as established players—would have to re-think about their strategy. They should be able to evolve solutions that align with consumer preferences. It should also be able to make the most of the data and technologies which is pertinent for digital identity. A BCG article focuses on some key features on how to create a robust identity solution[x]:

A holistic identity solution:

1. Takes into account actual consumer behavior
2. Provides right data at right time
3. Integrates data with robust infrastructure
4. Focuses on use-case approach
5. Evolves as per policy changes and new trends

Solutions should take into account actual consumer behavior. Most consumers have been able to show their discontent for filling in too many details for verifying their identity. They are mostly concerned about seeing their Facebook feed or just completing their purchase from an e-commerce website. Incorporating data and technology in the best way, providers should be able to create seamless user experience. Given a deep understanding of the customer behavior should be included in the solution design phase. Adopting the human-centered design could be one of the concepts – which are being incorporated by many technology companies[Xi]. The hallmark of this approach could be to make detailed observations on how users are able to interact with the systems as well as adjusting designs. Most organizations are able to put forth prototypes in front of the users – they scrutinize responses and make amendments. They repeat the process until the preferences and design is able to align in accordance to the corporate culture.

Platform should ensure providing access of right data at an appropriate time. Identity solution providers may work in the background by accessing various data that includes mobile phone data, behavioral analytics and biometrics to ascertain an identity without adding authentication burden on the user. However, it isn't an easy task to access accurate data from a plethora of data sources at an instant. Most useful type of data that

includes device IDs and biometrics might not be available widely. With this, some organizations might have acquired key sources, which would further limit the data availability.

Data should be integrated with robust capabilities as well as infrastructure. Advanced analytics is able to provide solutions to triangulate varied sources of data for authenticating identities. However, it might not be a simple task. Working along with many data types as well as determining identity needs accuracy and precision. It also requires right mix of processes and technology. In such a case, providers would have to invest in machine learning capabilities and AI. Simultaneously, they would also need to get a deep understanding of ML and AI, along with the analytics built around them. Occasionally, the model might be wrong or may not have enough information for authenticating. In such a case, the providers will need operational processes in which human intelligence might need to intervene and feed the data back into the model.

Providers might need flexible infrastructure which uses APIs for integration—that includes an ease of plug-and-play–data sources, and new sources which might be important in the future. For getting such flexibility, it would require significant investment as well as effort. This would need open, cloud-native architecture that will replace legacy IT systems, which is mostly inflexible. Providers could take steps that might help them with the ability of using new forms of data and then authenticate the identity.

Focus should be on use cases. In case of identity solutions that are industry- and country-specific and then are made on the parable of one-size-fits-all identity solution, it becomes a failure. Sample this, for banks they have to align by regulatory standards which do not apply to a retailer. Although, this doesn't signify that providers should limit themselves to specific markets. On the other hand, they should be able to broaden their platform over the period of time. Use-case approach is ideal here, as such an approach helps in integrating specific types of businesses —which includes financial institutions— for becoming an important participant in identity solutions.

Potential impact of policy changes and new trends should be considered. With new ideas gaining traction, digital identity would keep evolving with the advent of technologies and regulatory structures. Some of the recent developments that have impacted identity solutions include European Union's General Data Protection Regulation (GDPR), Aadhar program from India – that assigns every citizen with digital identification, California Privacy Act, and Cybersecurity law in China – that focuses on stringent requirements on transferring and using personal data outside the country of origin. In the meantime, concept that includes decentralized identity and self-sovereign identity, which focuses on providing control of personally identifiable information back to the individuals, have been emerging. These developments, and future trends, need to be taken into account while developing an identity solution.

3.2 Evolution of IAM systems

On the backdrop of the above challenges and requirements to create a robust identity solution, IAM technology needs to evolve as well. Moving to cloud, adopting microservices architectures, digitalization, along with growing cyber threats, have been expanding use cases for IAM. As per Mary Ruddy, Research Vice President at Gartner, here's how IT leaders may evolve their IAM systems for meeting new challenges[xii]:

Enhanced focus on security and fraud systems. Compromised credentials of users continue to be a major element in data breaches. As the number of breaches, that includes identity-related fraud, has been growing, enterprises should be able to evolve their systems to reduce system vulnerabilities. Reduce risk of identity breaches and fraud through robust authentication. Manage user identities by providing right access to the right resources, using adaptive policies to protect data, along with integrating IT security solutions such as MFA and endpoint encryption.

Provide support to higher levels of automation, along with increased communication between IAM modules. This will also include access management, administration and identity governance together with privileged access management.

Implement DevSecOps approach. DevSecOps helps in integrating security in the entire IT process right from the initial stages. This ensures that enterprises are able to address various security concerns and enhance its IAM modules on a proactive and consistent basis. With security embedded at each step, access regulations are being enforced across apps, APIs, data resources and microservices, resulting in minimizing the risk of data exposure. However, this will require changing the organizational mind-set, which is especially important for enterprises that have been developing their services and applications in-house.

Include customer's preferences and consent in customer data management policies. This is specifically necessary for meeting new and expanding privacy regulations, along with meeting expectations of the users.

EVOLUTION OF IAM SYSTEMS WILL ALSO DEPEND ON BEING A STEP-AHEAD IN DEVELOPING NEWER OR UPDATING EXISTING IAM TECHNOLOGIES, ALONG WITH FOCUSING ON A STRONG LEADERSHIP AND TEAM TO PROVIDE STRATEGIC INSIGHTS INTO CREATING A FLEXIBLE, YET ROBUST, IAM SYSTEM.

Role of adaptive access services to grow. One of the current trends in IAM is global use of analytics. Paul Rabinovich, Senior Director at Gartner believes that while, traditional adaptive authentication was mostly based on rules, the next generation adaptive access services is able to combine rules along with advanced analytics and machine learning[xiii].

Privileged access management (PAM) to become more critical. PAM is becoming one of the most critical security controls for securing enterprises. IT leaders are able to realize the value with PAM controls as it is able to reduce attack surface. However, reducing doesn't not mean eliminating the threat as in the most probable condition privileges might be hidden anywhere – such as administrative accounts, containers, system/service accounts, codes and devices. In order to find the threat, the system needs to manage accounts, together with reconsidering the structure of the operational model for privileged access within the enterprise.

IAM leadership to evolve. Transformation in digital world focuses on reinvention. IAM leaders would be able to collaborate with others in the business for orienting resources and people and ensuring that the IAM vision aligns with the goals of the enterprise as per digital transformation.

4. WHAT'S IN STORE FOR FUTURE? FUTURISTIC IAM INNOVATION

IAM technologies are increasingly evolving as per the accelerating scope of modern technologies. While the enterprises move to the cloud, adopt microservices and opt for decentralized identity, stringent data security and privacy regulations and constant cyber threats are resulting in the need for constant expansion of IAM technologies as well.

So how should one evaluate an identity solution or explore IAM technology in the coming years? Let's find out.

IAM to become more standard-driven. The industry is moving towards more standard-driven IAM technology such as FIDO or Fast identity online. Despite using password management tools, logging into an account often becomes a tiresome exercise. Users often find providing password, filling too much information and the entire process of online authentication a barrier. FIDO enables users to move beyond from managing their identity, by creating a seamless login experience through its fast-login feature across apps and websites. In fact, the set of protocols, FIDO 2.0, is allowing authentication to become passwordless, via Web Authentication (WebAuthn) API. This allows web apps to directly use public-key encryption and authenticators. Thus, IAM technology is also required to evolve as per the standards being followed in the industry. Furthermore, these standards will be required to be in-built into the IAM platform and will be seen as a mandatory practice, rather than an optional feature in the near future.

Adaptive authentication to follow MFA. As per Microsoft, one can reduce account compromise by 99.99 per cent with the use of Multi-factor authentication [xiv], however, minimal user adoption still remains a core concern area with around 90 per cent of Google users still not using two-factor authentication[xv]. Increased usability needs to be focused upon to make MFA mainstream, which

experts believe could be addressed through adaptive authentication, the next phase of MFA. With the deployment of adaptive authentication, the system would be able to access and decide which steps to initiate during the process of authentication, as per the risk profile and behavior of the user. Further, this enables the enterprise to undertake the precise level of gateway security for every login request, instead of undertaking the standard procedures required to be followed for each user, irrespective of the circumstances. Adaptive authentication, with the use of machine learning and identity intelligence, will also help in elevating the level of authentication. It will require consumers to use MFA only in the beginning, with the system, thereafter, to constantly monitor user behavior and prompt for two-factor authentication only in case of anomalous behavior.

System integrators to create holistic IAM systems. Enterprises are going beyond SSO and seen to implement holistic IAM solution – integrating access management, identity governance, privelege management, SIEM and other identity solutions. System intregators are seen to help by integrating different IAM products into one solution. Furthermore, building IAM solutions to secure endpoints is expected to pose a major challenge in the coming years. Experts are dubbing it as – "Exploding Endpoint Problem" – wherein, we would be expected to secure more than 1 trillion programmable endpoints within the next 20 years[xvi].

Regulatory compliances for data privacy continue to become stringent. With the implementation of GDPR and Payment service directive (PSD2), data protection and privacy regulations are expected to evolve and more stringent laws are likely to be implemented in the future as well. The California IoT Privacy Act and California Consumer Privacy Act (CCPA) are examples of such regulations. In order to support future guidelines, IAM platforms are required to be flexible and evolve as per the change in regulations.

Addressing microservice deployment challenges. Microservice depolyment is leading to creation of multiple entry-points, thereby, increasing security risk and system vulnerability. Each of the services need to include authentication and authorization feature in order to provide secure access to users, third-party apps and even other microservices. This challenge could be addressed through API Gateway, enabling users to enter into a system through a common entry-point, allowing them to use the microservices behind a secure firewall. One may further secure the access points and verify user's identity through OAuth 2.0 or JSON Web Token (JWT). In the near future, IAM providers will continue to create robust authentication and authorization techniques to provide right access to right users and protect user data, while providing seemless user experience.

Artificial Intelligence to define cyber security. Adoption of AI and ML technologies are significantly increasing in cyber security and for effective IAM implementation. In fact, the AI in cyber security market worldwide is expected to reach around USD 30.9 billion by 2025, as per a report by Zion Market Research[xvii].
While the current IAM technology is usually based on authenticating users against some pre-defined credentials, AI-driven authentication is more dynamic in nature due to the use of aural or visual clues. Going beyond biometrics, such AI-driven solutions will focus on establishing the identity of the users based on their appearance, along with their behavioral pattern, thereby, providing a potential for real-time security.

AVANCER'S EXPERTISE IN IAM

At Avancer, we understand that one of the compelling factors for organizations to bring in technical solutions is to adhere by existing compliances. However, there is so much more to technical solutions, and these add on benefits help in bringing efficiency, security and operational automation. We add an edge to solutions in Identity and Access Governance, IT Security and Big Data by closing any loopholes, and tailoring the solutions as per the needs of the business, industrial standards and regulatory considerations.

For more information on how we can make a difference in your organization, drop us a request here or directly contact our IT Security Leaders

RAJESH MITTAL, CTO| ARUN MEHTA, CEO | ABHA SHARMA, IT SECURITY EXPERT

Contact Us

Avancer Corporation
101 Interchange Plaza
Suite 201 Cranbury
NJ 08512, USA
Tel: +1 (609) 632-1285
Fax: +1 (877) 843-8594
Email: info@goavancer.com
Website: http://www.avancercorp.com/

To consult IAM Experts, click here.

[i] https://www.techrepublic.com/article/ai-adoption-40-of-company-leaders-have-no-hesitation/
[ii] https://www.bcg.com/publications/2019/digital-identity-solution-one-you-cannot-see.aspx .
[iii] a professional network for the information technology industry
[iv] https://www.spiceworks.com/marketing/public-cloud-trends/pdf-report/
[v] https://www.spiceworks.com/marketing/public-cloud-trends/pdf-report/
[vi] https://www.spiceworks.com/marketing/public-cloud-trends/pdf-report/
[vii] https://www.spiceworks.com/marketing/public-cloud-trends/pdf-report/
[viii] https://www.bcg.com/publications/2019/digital-identity-solution-one-you-cannot-see.aspx
[ix] https://www.gemalto.com/press/Pages/Social-media-companies-believed-to-be-vulnerable-with-61-of-consumers-saying-they-pose-greatest-risk-for-exposing-data.aspx
[x] https://www.bcg.com/publications/2019/digital-identity-solution-one-you-cannot-see.aspx
[xi] https://www.bcg.com/publications/2018/take-control-digital-future.aspx
[xii] https://www.gartner.com/smarterwithgartner/next-generation-trends-in-identity-and-access-management/
[xiii] https://www.gartner.com/smarterwithgartner/next-generation-trends-in-identity-and-access-management/
[xiv] https://www.microsoft.com/en-in/security/technology/identity-access-management
[xv] https://www.theverge.com/2018/1/23/16922500/gmail-users-two-factor-authentication-google
[xvi] https://thenewstack.io/the-exploding-endpoint-problem-why-everything-must-become-an-api/
[xvii] https://www.zionmarketresearch.com/report/artificial-intelligence-in-cyber-security-market