AUJAS CYBERSECURITY | NSE NSEIT

FROST & SULLIVAN

ROBOTICS DRIVEN AUTOMATION FOR SMARTER IDENTITY AND ACCESS MANAGEMENT SOLUTIONS

The potential that Robotics Process Automation (RPA) promises to bring in through simplification of IAM processes is a commendable advantage to deal with enterprise security, governance and compliance challenges. RPA brings down manual intervention by automating routine tasks and building an integrated platform.

Enterprises have been investing relentlessly in technologies to address the changing business landscape. The focus remains accelerated business growth driven by processes, competencies and operating models. With the larger aim of bringing in digitalization within enterprises to address the need of customers, chief digital security officers realize the value of Identity and Access Management solutions to manage the resources across the diverse technology sets.

An Identity and Access Management (IAM) solution is central to building a connected workplace where information sharing is liberal yet needs close monitoring and user restrictions. A modern enterprise ecosystem consists of stakeholders who not only belong to the employee community but also outsiders who need access to corporate databases and applications on a regular basis. With vendors, suppliers and customers all becoming an integral part of the overall value chain, having a distinct enterprise perimeter does not work in most cases as organizations move their applications and workloads to the Cloud and in a business environment where there is a heterogeneous mix of the user and technology element, managing user identities and access privileges becomes a prime imperative.

The next level of conversation within enterprises is centered around empowering employees with digital technologies; Identity and Access Management becomes a foundational element of any security program

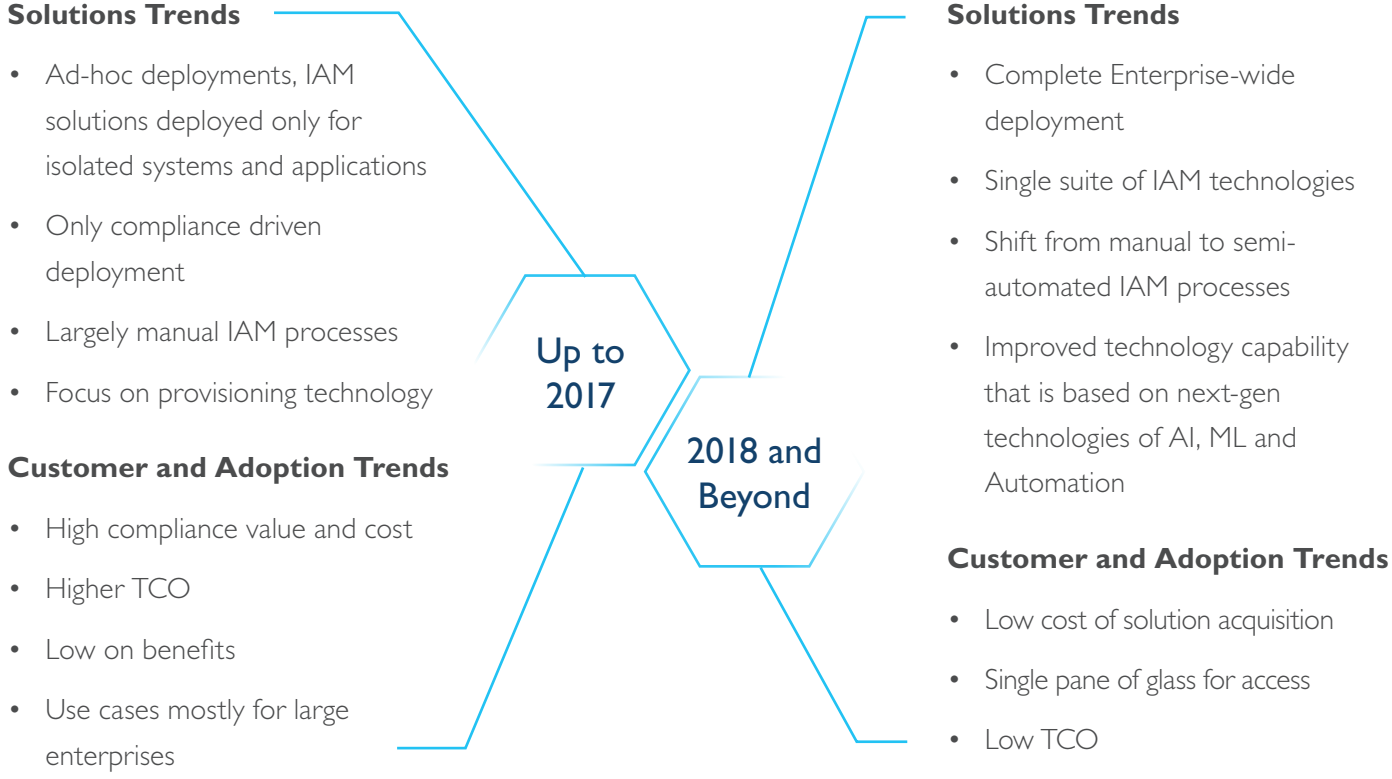
THE MOVE TOWARD **NEXT GENERATION IAM SOLUTIONS**

IAM as a technology concept was initially started to address the need of access management and related compliance needs. The deployments that happened earlier across enterprises were largely ad-hoc and project based. Network administrators considered using an IAM solution only for providing provisioning rights for isolated systems. However, given the high cost of the solutions, enterprises failed to lower the TCO and make it an enterprise wide solution.

IAM solutions evolved over time, nonetheless were challenged with simplicity, automation, integration capability and operational efficiency

The next wave of IAM solutions saw deployments being made across the enterprise. Organizations realized the need to replace mundane job processes to avoid human error and improve efficiency. IAM became a part of overall enterprise strategy, which included every type of user. With an aim to develop more intelligent solutions, IAM vendors started imbibing next-generation technologies like automation into products. A single product that caters to all enterprise needs from compliance requirements to identity management, access certification and infrastructure management was developed that created better value proposition. The best IAM solutions would have a single pane of glass for access management with seamless integration with existing technologies and minimum human intervention.

Exhibit 1: The shift toward an Automated IAM Solution



Source: Frost & Sullivan

WHY LEGACY IAM SYSTEMS FAIL TO WORK IN TODAY'S CONTEXT?

Enterprises do understand the value of IAM solutions. They have been using such solutions for quite some time; however, have not reaped benefits to a large extent. Security breaches happen frequently due to inability of the traditional IAM solutions to deal with today's enterprise needs.

Listed below are the challenges enterprises deal on a regular basis while handling IAM solutions:

Exhibit 2: Top 5 Drawbacks of Traditional IAM Solutions

01

IAM SOLUTIONS NOT MEANT FOR TODAY'S HETEROGENEOUS IT INFRASTRUCTURE

The modern enterprise infrastructure includes Cloud Applications, Virtualization, Software Defined Architectures, etc. which makes it difficult for enterprises to manage identities

02

LIMITED INTEGRATION CAPABILITY

Enterprises find it challenging to integrate IAM solutions with existing IT infrastructure

03

TIME CONSUMING

Most traditional IAM solutions are time consuming; the on-boarding and off-boarding process becomes a challenge and employees don't get access to applications needed to perform their jobs on time

04

REQUIRES HIGH LEVEL OF HUMAN INTERVENTION

Traditional IAM solutions require resources to manually define and process Identity and Access Management norms which becomes a daunting task when it comes to large and diverse organizations

05

COMPLEX USER INTERFACE

Most IAM solutions have a complex user interface which makes it difficult for Security Professionals to take advantage of the solution

Source: Frost & Sullivan

To deal with these aforementioned challenges, enterprises resorted to multiple ways of IAM deployment. This includes semi-automatic IAM systems, use of file transfer based integrations and functionality compromises. While, these solutions help ease IAM processes to a certain extent, enterprises still could not completely benefit from these deployments.

Exhibit 3: Operational Challenges of Commonly used IAM Deployments

DEPLOYMENT MODEL	CHALLENGE
SEMI-AUTOMATIC IAM SYSTEMS	Use of manual teams along with workflow engine for access provisioning/deprovisioning
USE OF FILE TRANSFER BASED INTEGRATIONS	Good from a compliance perspective but not ideal for risk mitigation or efficiency
FUNCTIONALITY COMPROMISE	Focused on access review but not for access provisioning

Source: Frost & Sullivan

BUILDING SMART IAM SOLUTIONS: **THE TRANSITION TOWARD ROBOTICS DRIVEN AUTOMATION**

THE NEED TO AUTOMATE

IAM solutions have been fast evolving to help organizations meet the needs and expectations of enterprises. User actions like viewing or editing a document need to be closely monitored depending on the role of the individual within the organization. Features like Single Sign On (SSO), Multifactor Authentication (MFA), Lifecycle Management, Governance and Privileged Access Management (PAM) have become a frequent activity for managers. Methodologies like Provisioning, De-provisioning, Directories, Authentication, Authorization and Auditing are being used for Identity and Access Management purposes. The need to simplify these frequently used processes has been realized and enterprises are looking to automation as an easy way out. Automation helps IT teams create and manage identities and avoid manual error.

Exhibit 4: Why to Automate IAM Processes

- Limit manual intervention and error
- Ease up IAM processes by simplifying tasks
- Excellent for fast changing identity and access requirements within enterprises
- Ensure streamline operations
- Build Just-in-Time IT Systems
- Better manageability of Employee Lifecycle, Process Requests, SSO, MFA, Password Management, etc.
- Highly scalable and flexible

Source: Frost & Sullivan

THE ADVANTAGES OF ROBOTICS DRIVEN IAM

Robotics Process Automation (RPA) mimics human behavior to perform routine human tasks which otherwise require lot of human energy. It helps automate IAM processes that are repetitive, rule based and do not require human intelligence. The IAM system uses software that recreates repetitive steps by pulling out information from one system and takes action based on user request, data and expected outcome.

Identity Governance and Administration (IGA) is another area which benefits from RPA. Functions in IGA like provisioning/deprovisioning, password management, role and access management, certification, which are traditionally manual, often work in isolation. Putting connectors across all of these is a daunting task which requires heavy investment. Siloed processes are error prone and expose enterprises to a cyber-attack. Use of RPA helps streamline multiple identity governance processes by building a centralized platform and talking care of the overall compliance, security and risk posture.

Exhibit 5: Difference between Traditional IAM and Robotics Driven IAM

TRADITIONAL IAM	ROBOTICS DRIVEN IAM
Takes a discrete approach toward Identity and Access Management	*Takes a platform approach that addresses the need of identity management, access certification, infrastructure management and compliance*
Repetitive coding	*Code once*
Manual Configuration	*Auto configuration generation*
Doesn't function in a heterogeneous IT infrastructure	*Suited for modern infrastructure which includes Cloud, Virtualization and Software Defined architectures*
Complicated processes with high manual intervention	*Easy on-boarding and Life Cycle Management*

Source: Frost & Sullivan

CHOOSING THE RIGHT IAM SOLUTION

To unsheathe the benefits of RPA in IAM processes, it is important that enterprises partner with the right service provider. IAM is an integral part of the security strategy and choosing an IAM solution that addresses the need of organizations is fundamental. It should be ensured that the IAM solution should have useful functions like MFA, One-time Password (OTP), third-party vendor access management and monitoring and shared account personalization features for administrators. The solution should have proactive incident response capability for an event of identity or access breach. Compatibility is a common challenge and the IAM solution that is chosen should integrate with network architectures, operating systems and SIEM systems used by the organization.

With innovations replacing traditional IAM solutions, vendors have equipped themselves with latest technology sets like RPA and Threat Intelligence. This gives an excellent opportunity for customers to bank on these vendors who understand enterprise challenges and work together by using next-generation technologies. Solutions should be user friendly automating repetitive jobs only to reduce human intervention and error percentages.

An IAM solution driven by RPA is an invention that makes Identity and Access Management dependable for enterprises.

Exhibit 6: Key Questions to Ask while Selecting an IAM Solution

How critical is an IAM solution for Enterprise and how can we benefit from the latest innovations in IAM?
What applications do we need our IAM solution to integrate with or support?
Do we need to use an On-premise, Cloud or Hybrid Solution?
Can we scale up/down the solution as per our needs and is the solution ready to cater to the fast changing technology landscape?

Source: Frost & Sullivan

> ***Enterprises should not merely select an IAM vendor but partner with a provider who builds their solution based on next-gen technologies that automate processes and minimize manual involvement***

ROBOTICS DRIVEN IAM **FROM AUJAS**

Aujas is one of the fastest growing cyber security firms in the world. It has been instrumental in working closely with customers to build and transform cyber-security posture to enable business and mitigate risks. The company's focus on strengthening security resilience by reducing the consequence of attacks, threats and risks has earned confidence among enterprises. Driven by a strong leadership team who understands and tracks the cyber-security market closely, Aujas has been working relentlessly to protect businesses.

In the process of working with enterprises over the last few years, Aujas has comprehended the various challenges that organizations have to face regularly. CISOs have been struggling to minimize human error within IAM processes. Efficiency has always been questioned; siloed processes have mostly been missing. Repetitive tasks are being performed by human beings which is a loss of time and effort. To address these challenges, Aujas has introduced the power of RPA in IAM solutions.

Today, the narrative is built around "IAM with Robots". Routine tasks are being automated making it easier to provide identity and access control along with better governance. Aujas starts by classifying applications in accordance with the level of integration that is needed with IAM. This is in turn a function of ease of integration, number of users and business/compliance criticality. Based on this function, the team decides the optimal level of application integration needed.

As a part of quick application onboarding, Aujas utilizes the assembly line approach (see exhibit below) for integration of applications. It uses automation for requirement processing and configuration upload with failsafe manual methods. Aujas in partnership with Sailpoint has been working toward introducing capabilities for setting up a native integration factory.

Exhibit 7: IAM Rapid Application Onboarding; the assembly line approach for integration of applications

01	02	03	04	05	06
Uncategorized Apps	**Requirement Gathering and Processing**	**Configuration Upload**	**Confirm Reconciliation**	**Independent Testing**	**Production Ready Integrations**
SailPoint based SAM linked Bronze Other Apps	RA Directly from PALM RA from existing Integrations	METHOD 1 PALM API based export to Sailpoint (subject to version limitations) METHOD 2 PALM xml compatible with Sailpoint UI based setup METHOD 3 PALM export for UI based import into Sailpoint			

Source: Aujas

Aujas leverages an integration factory approach using Platform for Access Lifecycle Management (PALM) to achieve application onboarding goals. In this approach, every app goes through standardized tasks much like components in a factory assembly line.

The IAM Application integration factory brings in assembly line predictability, efficiency and automation to the process of integration of applications with IAM systems. The IAM Integration Factory has been used to expedite the integration process by 5x on an average. The Integration Factory is a set of processes, methodology and tools that can be utilized with various IAG solution environments.

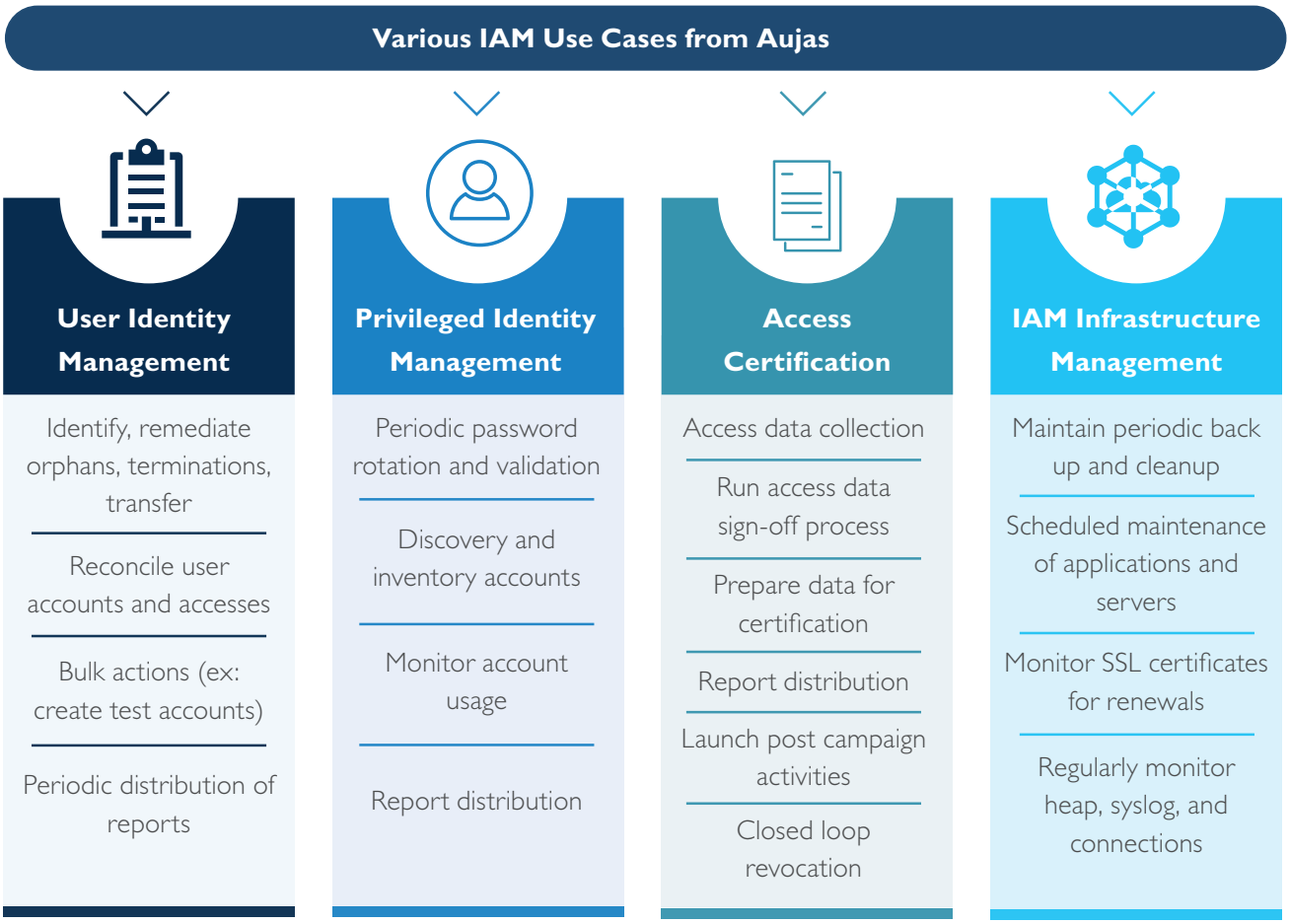
The IAM integration factory has now become Aujas' default approach for app integration for any initiative with more than 50 apps in scope. The company uses this approach to/for:

- Complete role profiling for enterprise apps
- Generating access packets
- Capturing workflow requirements
- Robotics integration
- Auto-generation of IAM code
- Manual validation by engineers

THE SOLUTION OVERVIEW

Enterprises need to adopt IAM solutions to move beyond compliance and address the pressing need for identity management, access certification and infrastructure management

Exhibit 8: IAM use-cases for Robotics Driven IAM



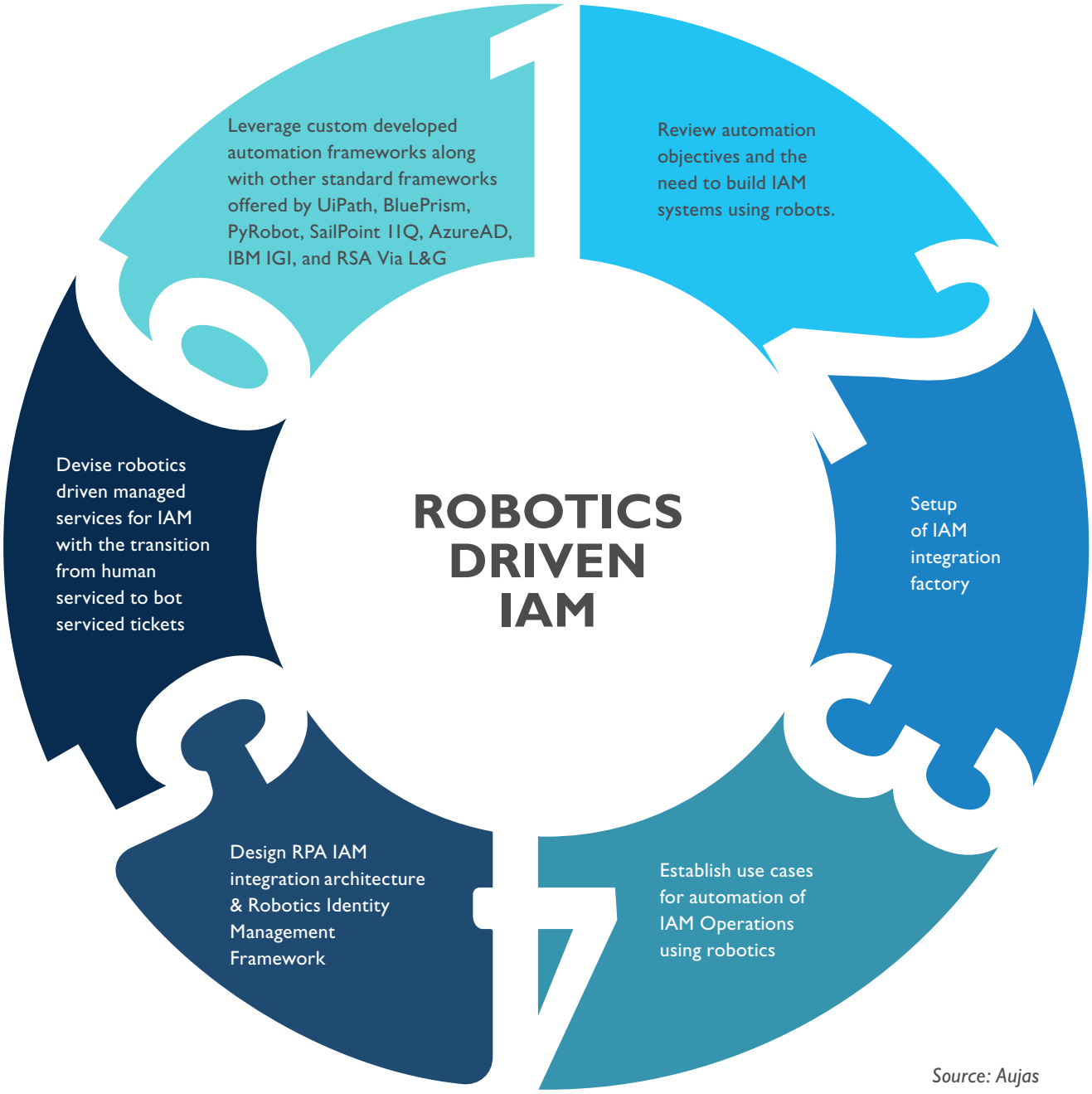
Source: Aujas

Aujas IAM solutions are highly automated which help in faster integration with businesses enabling operational efficiency and better cost management. The solution does not use product level connectors or adopters which are expensive and instead uses robotics to automate and link IAM tasks to address the growing need of user identity and access requests. Aujas IAM solutions leverage automated rule based techniques to deal with repetitive tasks and eliminate human error.

Aujas Robotics Driven IAM finds excellent use cases within enterprises. Companies are often challenged by the need to have a unified and standard method for access request. Business wants cost effective compliance and de-risking by auto de-provisioning. The larger goal

remains quick deployment of IAM solutions and elimination of manual operations. Aujas provide enterprises with a unified platform for access request management, auto generation of app request forms, auto deprovisioning, RPA driven IAM provisioning ops and audit trails for easy compliance checks. These help enterprises to digitalize and standardize approval processes by eliminating human errors. Outcome is fast as the solution is made live within 100 days for 100 applications against traditional timelines of years. Robotics Driven IAM from Aujas is endpoint independent and meant for a large variety of applications.

Exhibit 9: Aujas Robotics Driven IAM Process



Source: Aujas

THE UNIQUE DIFFERENTIATOR AND VALUE PROPOSITION

The expertise and experience that Aujas as a company brings to customers is considerably unique.
The Integration Factory approach used by Aujas PALM provides up to 85% efficient app integration for enterprises. PALM syncs well with other systems in the enterprise ecosystem, is workflow driven and furnishes accurate dashboard, statistics and reporting. Rapid integration approach with PALM solution takes around 16 days of analysis and 2 days of IAM configuration development.

Aujas takes into consideration a multi-track approach for the transition plan. The entire transition phase comprises multiple parallel tracks where critical elements like current questionnaire, current internal CSAT, description writing standards, etc. are being analyzed. The transition phase is governed and executed by an experienced team of Onsite Tech-leads, Off-Shore Project Managers, Business Analysts and Lead Engineers. Aujas' unique differentiator lies in the seamless IAM onboarding and integration experience that it offers to global enterprises. The company has over 130+IAM practitioners with implementation experience using specific IAM products. The team has the capability to deliver hybrid-onsite and remote service delivery. The company runs an IAM Center of Excellence (CoE) to drive innovation. Aujas is technology versatile with strong partnerships with all leading IGA, Access Management, Privileged Identity Management (PIM) and Full Suite IAM vendors.

THE WAY FORWARD **IN IAM**

The future of Robotics Driven IAM would involve cognitive technologies like Machine Learning (ML), Speech Recognition and Natural Language Processing (NLP). Robotics is likely to imitate human behavior and over time become more accurate, faster and foolproof. Human intervention would be further reduced and efficiency would reach newer heights. Analytics combined with AI would provide contextual insights into breach management thereby strengthening Identity and Access Management processes. While complete automation is not possible today, the future of IAM would be built around next generation technologies thereby making enterprises ***"Go Smarter"***.

> *Artificial Intelligence would transform IAM into an intelligent security solution and change the way user identity and access privileges are being managed, monitored and controlled*

ABOUT FROST & SULLIVAN

For over five decades, Frost & Sullivan has become world-renowned for its role in helping investors, corporate leaders and governments navigate economic changes and identify disruptive technologies, Mega Trends, new business models and companies to action, resulting in a continuous flow of growth opportunities to drive future success. Contact us: Start the discussion.

www.frost.com

ABOUT AUJAS CYBERSECURITY

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

For more information, do visit us at www.aujas.com You can also write to us at contact@aujas.com