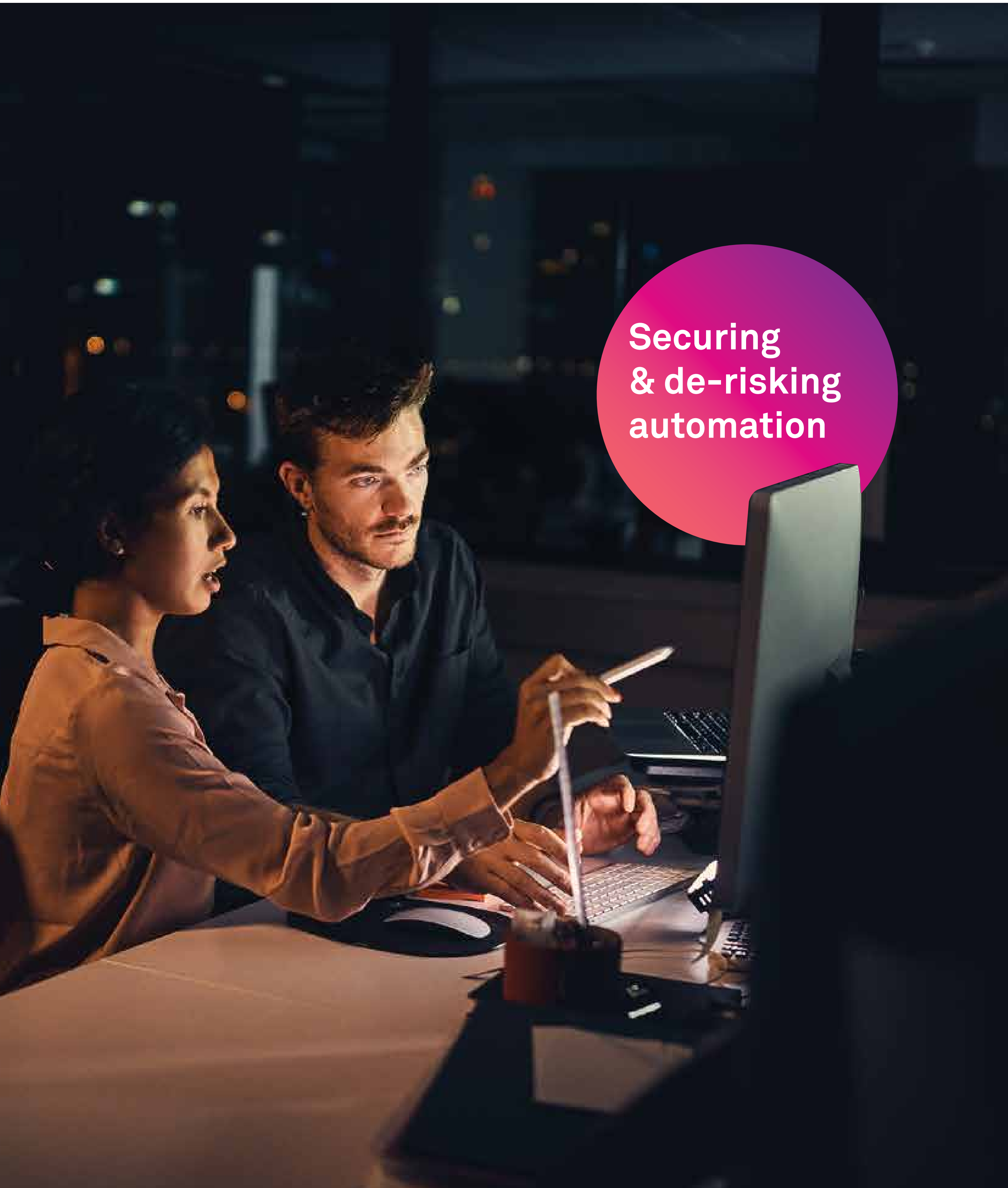
wipro holmes

wipro



Securing & de-risking automation

As per Mordor intelligence PROCESS AUTOMATION MARKET - GROWTH, TRENDS, AND FORECAST (2020 - 2025) study 'The process automation market was valued at USD 76.83 billion in 2019 and is expected to reach USD 114.17 billion by 2025, at a CAGR of 7.23% over the forecast period 2020 – 2025'[1]. While RPA products have matured and are widely accepted, customers are also looking at automating end to end IT processes, beyond RPA, from simple task-based automation to Cognitive Automation, to provide better customer experience and improve operational efficiencies. With digital transformation being a top priority for the enterprise CxO, and automation being central to this transformation, the focus on automation has been like never before. But automation comes with its own challenges and risks, and if not handled and implemented correctly, may result in a nightmare, rather than being a saviour.

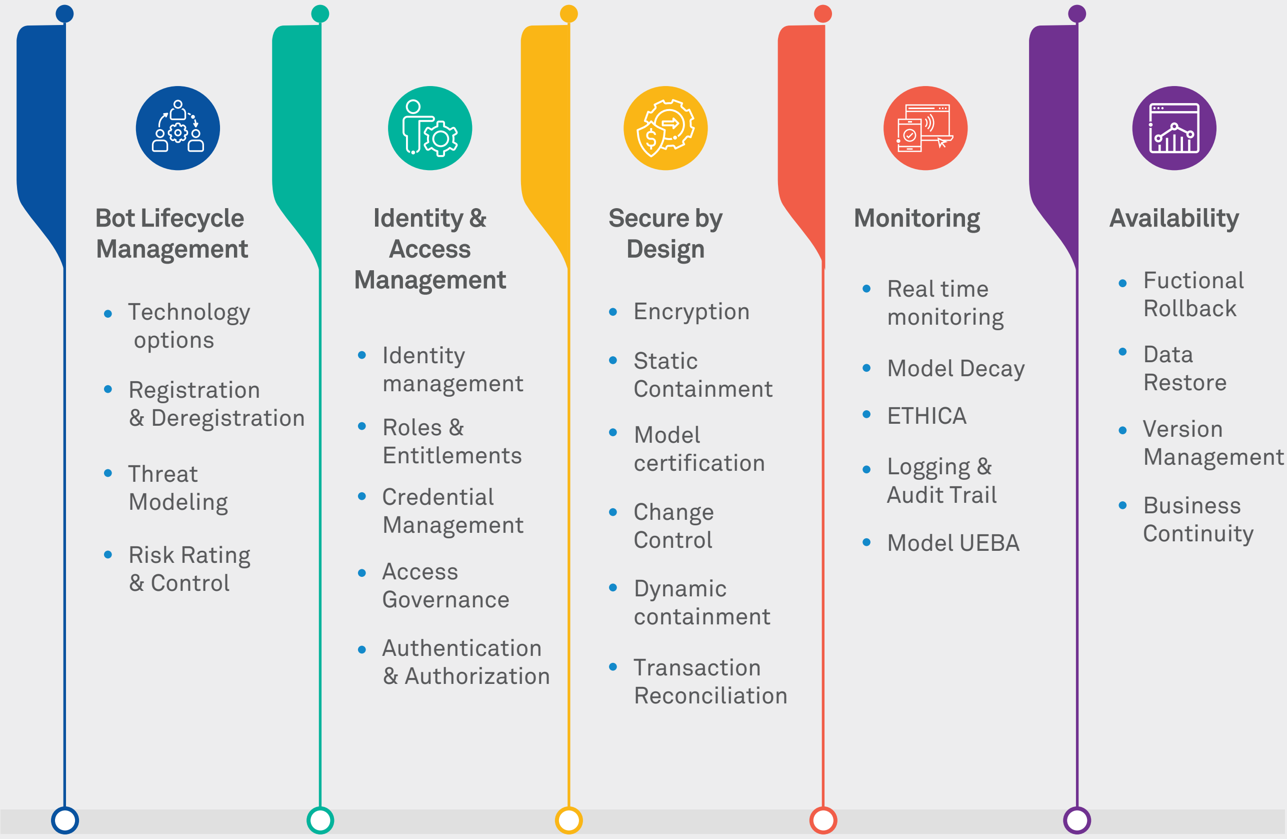
Security risks and challenges in adopting and scaling automation:

Automation helps organizations in delivering better efficiency as well as experience. As part of their digital transformation journey, organizations are focusing on end to end business process automation and IT process automation. This automation adoption can be a double-edged sword and brings significant risks. For e.g., in one such case in January 2017, Delta told investors that one glitch in their automated system caused a widespread outage, costing the airline more than $150 million[2]. As evident from this example; these risks affect companies financially and also impact their reputation and credibility. With the increased use of such automation programs (or bots), there are also growing concerns about the misuse of automation. This misuse can range from compromising credentials to getting access to environment or making unauthorized changes which impact the functionality, to a sophisticated one like introducing biases in case of Cognitive automation, impacting and influencing the decisions taken by such Bots. Such cases have caused apprehensions in the mind of business units where automation is being adopted and has slowed down the process considerably.

To cater to these challenges and safeguard automation bots from any misuse, there is an immense need for a comprehensive automation governance framework to ensure such challenges are identified in advance, and corrective measures are taken, so that interests of an organization are safeguarded, and it can adopt automation at scale.

A high-level overview of this governance framework is shown in figure 1.

To cater to the challenges and safeguard automation bots from any misuse, there is an immense need for a comprehensive automation governance framework to ensure such challenges are identified in advance, and suitable corrective measures are taken.



Bot Lifecycle Management

- Technology options
- Registration & Deregistration
- Threat Modeling
- Risk Rating & Control

Identity & Access Management

- Identity management
- Roles & Entitlements
- Credential Management
- Access Governance
- Authentication & Authorization

Secure by Design

- Encryption
- Static Containment
- Model certification
- Change Control
- Dynamic containment
- Transaction Reconciliation

Monitoring

- Real time monitoring
- Model Decay
- ETHICA
- Logging & Audit Trail
- Model UEBA

Availability

- Fuctional Rollback
- Data Restore
- Version Management
- Business Continuity

Figure 1: Bot Governance – high level experiential architecture

Bot lifecycle management: The governance solution should have the capability to manage the end-to-end bot lifecycle, covering aspects like bot onboarding, technology choices, registration and deregistration, Risk rating and control mechanism and bot reuse, etc. It would also include the lifecycle management of the AI model deployed as part of the bot. The critical aspect of this lifecycle is threat modeling, which allows organization to identify the potential threats and drive the risk ratings and corresponding controls. A suitable lifecycle management process will ensure that an approved, secured and robust mechanism is adopted.

Identity and access management: With the increasing adoption of pervasive automation, bots would provide more in-depth access to systems—as a result, identification and accesses for bots must be managed appropriately and centrally.This would include capabilities like identity management, authentication and authorization, credential management, roles and entitlements, segregation of duties, access verification and reconciliation as well as access governance.

Secure by design: One of the key aspects of ensuring confidence in automation is around built-in security. It's incredibly pertinent to take security considerations while designing the Bot, ensuring that critical aspects like data security and privacy, auditing, transparency, explainability, etc. are factored in. Apart from these features, Bot design should also have containment mechanisms built-in - both static as well as dynamic in nature. In addition, features like model/bot certification, change control, auditing and transaction reconciliation, vulnerability & penetration testing , etc. should also be considered while developing an automation bot. Some of these features can be as simple as limiting the number of transactions in a day or complex ones like mechanisms to ensure that solution is not doing anything unintended dynamically, and any deviation from the regular intended steps can be contained immediately. In the healthcare industry, 21 CFR Part 11 compliance is one such example that can be adopted. Despite these checks in place, there are functions within an organization that are reluctant to adopt automation, given the sensitive nature of the process and data involved, a case in point being automation related to the financial domain. In such cases, it is pertinent that each transaction is reconciled, clearly showcasing the integrity and accuracy of such transactions, and slowly once the confidence builds up, automation Bots are rolled out.

Monitoring: With pervasive automation, digital workers are accessing the core systems, and it's important to ensure that necessary monitoring is in place to prevent any unwarranted events. Like any other monitored solution, automation solution also needs to be continuously monitored and audited to ensure compliance and adherence to the expected behavior. For cognitive automation, the monitoring should be much more in-depth, looking at essential facets like model decay, precision, accuracy, explainability, and any new biases to ensure that automation is working in line with the organization's policies and also adhering to the regulatory and legal compliances. The monitoring systems should be able to proactively identify the possibility of an adverse event and immediately take the required corrective actions while notifying the required teams. The monitoring process also needs to constantly evolve, keeping up with the changing landscape and ensuring control and adherence.

Availability: With security, monitoring and containment controls in place, the function and service owner would still like to understand the contingency plan in case something goes wrong. Availability solution addresses this need and ensures the functional rollback and data correction are done as required. Automation solutions need to have an inbuilt ability to identify the changes made on the data and reverse them; if anything untoward is observed.

The automation solution, without taking into consideration availability aspects, would be incomplete and extremely risky.

Conclusion:

As digital workers in the form of various bots become pervasive in the enterprise, it's important to ensure they have governance frameworks and tools to monitor the work done by these digital workers. Apart from monitoring, these solutions needs to be secured during the design process and must be coupled with availability solutions, in case things go wrong. Having these frameworks in place will help in addressing the adoption and scalability challenges and expedite the digital transformation journey while ensuring adherence to compliances and risk mitigation.

References:

https://www.mordorintelligence.com/industry-reports/global-process-automation-market-industry

https://www.csoonline.com/article/3188426/the-7-worst-automation-failures.html

About the authors

Vaibhav Bakshi
Consultant- AI and Automation,
Wipro HOLMES™

Vaibhav leads New Solution Definition function for Wipro HOLMES™. With over two decades of experience in the industry across functions such as Consulting, Program Management, Engineering, Solution Architecture and Service Delivery, Vaibhav specializes in delivering business outcomes using AI & Automation. He has delivered these solutions across multiple manufacturing and technology customers across the globe.

Nikhil Mehta
Lead Architect – Wipro HOLMES™

Nikhil is the Product Owner of Wipro HOLMES™ AIOps in the "HOLMES for IT" product line. With 16+ years of industry experience, he has played a pivotal role in setting up and developing AI product lines on the Wipro HOLMES™ AI platform. He has successfully delivered AI-enabled IT transformations focused on responding to IT operations, improving performance and supporting growth. Nikhil has played various roles across multiple business functions like Product Engineering, Product Management, and Service Delivery; with expertise in defining, building and deploying solutions across multiple domains such as Logistics, Telecommunications, Supply Chain and Retail.

Wipro Limited
Doddakannelli, Sarjapur Road,
Bangalore-560 035,
India

Tel: +91 (80) 2844 0011
Fax: +91 (80) 2844 0256
wipro.com

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading global information technology, consulting and business process services company. We harness the power of cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies to help our clients adapt to the digital world and make them successful. A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, we have over 175,000 dedicated employees serving clients across six continents. Together, we discover ideas and connect the dots to build a better and a bold new future.

For more information,
please write to us at
info@wipro.com