WHITE PAPER

Security Risks using generic IDs with RPA bots

Raghu Boddu
CISA, CFE, CDPSE
Managing Director - ToggleNow

TOGGLENOW®

Overview

As businesses seek to streamline operations and increase productivity, automation has become an indispensable tool in enterprise resource planning (ERP) systems like SAP. The use of bots — software applications that run automated tasks to simplify various activities — has rapidly expanded within SAP environments.

From automating data entry to performing routine maintenance checks and processing complex transactions, bots have transformed SAP's functionality, offering a significant reduction in manual effort, greater speed, and enhanced accuracy. Yet, with these benefits come a range of challenges and risks that organizations must address to implement bots effectively and securely.

This paper explores the landscape of bot usage in SAP systems, delving into the technical, operational, and security challenges that emerge as businesses adopt this technology. While bots present opportunities to enhance SAP processes, they also introduce risks related to system integrity, data privacy, compliance, and cybersecurity. Many organizations are finding that a robust framework for governance and risk management is essential to navigate these risks and make the most of what bots can offer in the SAP ecosystem.

The Team

Here is the team that contributed to the development of this white paper.

Raghu Boddu

Managing Director

As Managing Director of ToggleNow, Raghu Boddu oversees strategic growth, drives SAP innovations, and ensures excellence in project delivery. He leads a team to deliver cutting-edge solutions in SAP Security, GRC, and automation.

Santosh Nasine

Director - Sales & Operations

As Director of Sales & Operations at ToggleNow, Santosh focuses on optimizing processes, ensuring efficient resource management, and delivering high-quality SAP solutions. He drives operational excellence to meet client expectations and sustain business growth.

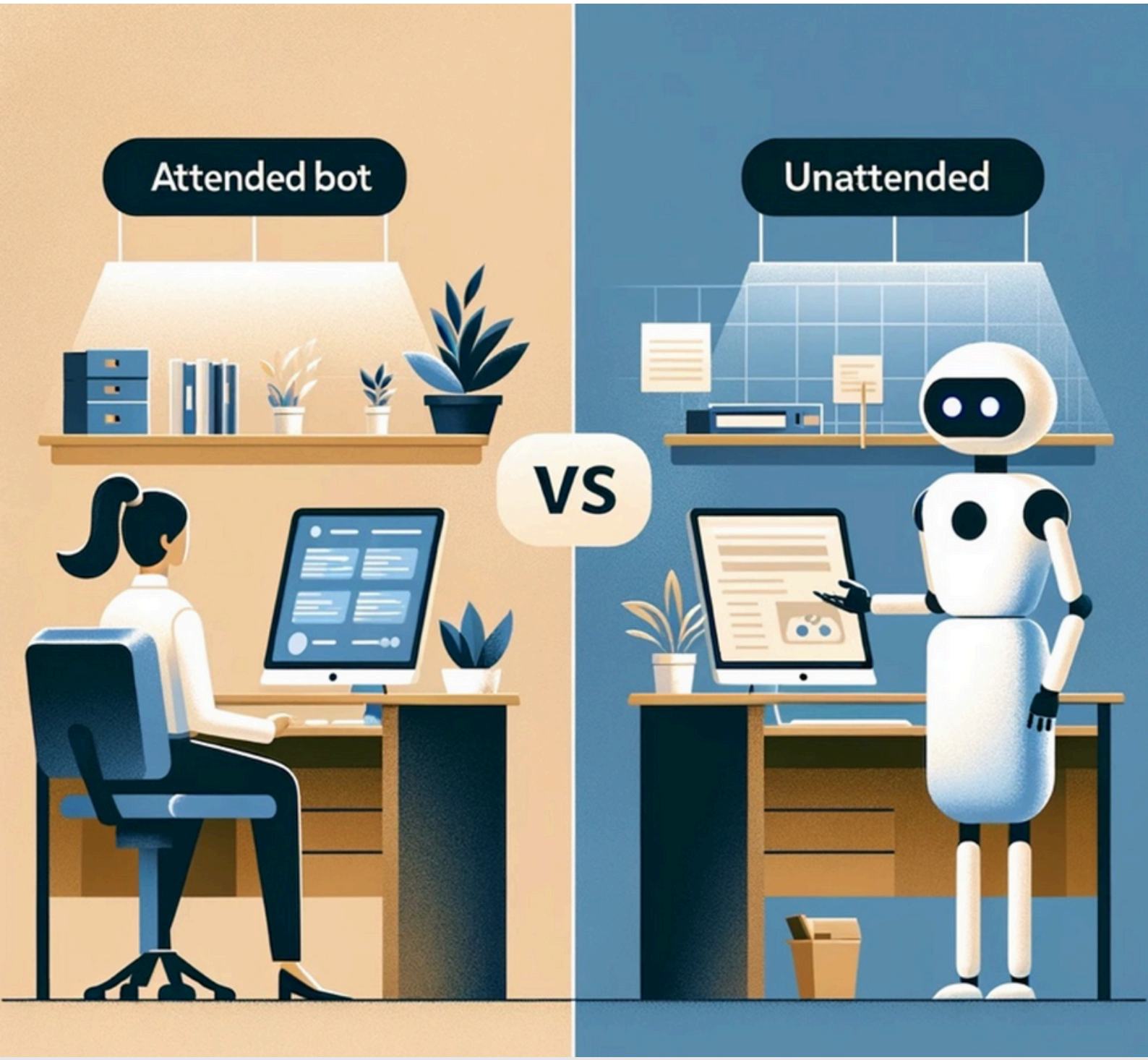
Drishti Nashine

Advisor – Security and Audit

As Advisor – Security and Audit at ToggleNow, Drishti provides strategic guidance on SAP security frameworks and audit compliance. She ensures robust governance and risk management to enhance system integrity and safeguard client operations.

Types of BOTs

It's great to learn about the different types of bots.



Attended vs Unattended

Attended and unattended bots represent two distinct approaches to automation in SAP environments, each catering to different operational needs. Attended bots are designed to work alongside human users, assisting them in performing tasks as they're needed in real time. These bots are typically triggered by user actions and are ideal for scenarios where human judgment is essential or where the bot supports specific, user-driven workflows. For instance, an attended bot might be used to speed up PR creation by recording the steps and then executing it with data in spreadsheets.

By handling routine, time-consuming tasks, attended bots allow employees to focus on more complex responsibilities, enhancing both productivity and user experience.

Unattended bots, on the other hand, operate autonomously in the background without human intervention. They are typically scheduled or event-driven, handling repetitive, rule-based processes at scale, such as batch data processing, report generation, or system monitoring tasks in SAP. These bots excel in executing high-volume transactions and tasks that don't require real-time human oversight, maximizing efficiency and freeing employees from routine operations. While unattended bots can provide significant cost savings, they also require robust governance, as improper configurations or security gaps can introduce risks. Both types of bots have unique roles within SAP, and organizations must carefully select the appropriate bot type based on process requirements and risk considerations to achieve optimal results.

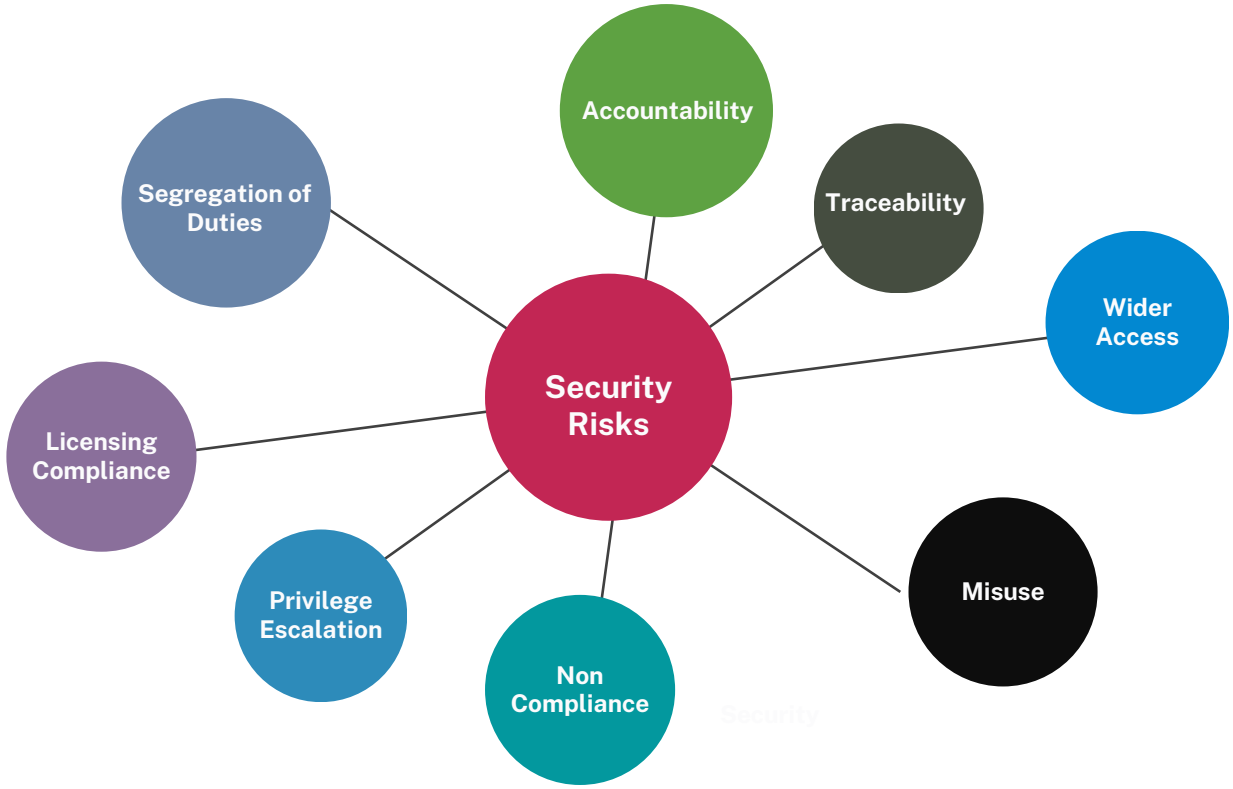
Here's a quick comparison between attended and unattended bots:

Attended vs Unattended

FEATURE	ATTENDED	UNATTENDED
HUMAN INTERACTION	Requires real-time human interaction	Operates without human intervention
TRIGGER MECHANISM	User-triggered (e.g., initiated by employee action)	Scheduled or event-driven
USE CASE	Supports tasks needing human judgment (e.g., customer support)	Automates repetitive, high-volume tasks (e.g., data processing)
OPERATIONAL SCOPE	Primarily supports individual users or small teams	Scales to larger, enterprise-wide processes
BENEFITS	Enhances user productivity and supports decision-making	Maximizes efficiency and reduces operational costs
RISK CONSIDERATIONS	Requires strict governance to prevent security and compliance issues.	Minimal risk as the BOTs are process driven

Security Risks – What organizations must consider?

As organizations adopt bots to automate SAP processes, they often face several challenges, especially around security and user identity management. One of the key issues is the use of user IDs to utilize bots, which presents unique risks to system integrity, data security, and compliance. Here are some of the key challenges:



BOTs typically require access to sensitive systems and data. When using attended BOTs, many organizations provide generic IDs for bots as these IDs are often shared across multiple people, making it difficult to trace individual actions or pinpoint the origin of potential security breaches. This lack of accountability creates opportunities for malicious actors to exploit vulnerabilities in the system.

How to address this risk?

When implementing bots in SAP, ensuring secure and compliant access is crucial to mitigating risks related to user identities and Segregation of Duties (SoD). Bots often require specific access rights to perform tasks autonomously, but assigning generic user IDs to bots introduces security and compliance vulnerabilities. Here are some recommendations:

Instead of creating generic IDs for each bot, user ID should be linked to an accountable individual to ensure clear ownership and traceability of actions. This linkage helps prevent unauthorized activities and ensures that actions taken by bots can be tracked to responsible personnel if needed.

By assigning necessary permissions to business users, who can then utilize the bots without sharing or reusing user IDs. This approach preserves accountability and aligns with SoD principles by limiting access to conflicting tasks within the system.

Ensuring SoD compliance is essential—if business users are given one set of access rights and the bot has access to conflicting rights through a generic ID, it could lead to potential SoD violations and insider threats. By assigning clear access roles, performing regular SoD checks, and avoiding generic IDs, organizations can better control bot activities, safeguarding both system integrity and compliance.

Bots, if not carefully managed, can be prone to misuse. Many organizations use Service type user IDs, instead of Dialog IDs to avoid:

- Resetting the password reset
- Additional license costs/requirements
- Minimize SoD requirements

Did you know that this can inadvertently create vulnerabilities in the system? For example, if a bot is compromised, the attacker can gain broad access to SAP resources, potentially impacting the entire organization. Additionally, bots may sometimes be given more privileges than necessary, leading to potential misuse of system access.

How to address this risk?

NOTE: Using Service type user IDs, and sharing the username and password to a team of individuals will increase the potential SoD violations and insider threats.

Service-type user IDs are typically generic, shared accounts that do not reflect the individual bot or user performing an action. As a result, it becomes challenging to track and audit the activities carried out by bots. This lack of traceability can lead to compliance issues, especially in highly regulated industries, where auditors and regulators require a clear record of system interactions and data manipulation.

The common mistake - Over provisioning - What it is?

Managing roles and authorizations for bots is inherently more complex than for human users. Administrators often create and assign wider access to Bots to ensure smooth execution of tasks, which can lead to “overprovisioning” and increased risk exposure. Ensuring that bots are assigned the least privileges is critical.

Non-Compliance with Security Policies

Service-type user IDs often bypass strict authentication protocols and audit requirements. In highly regulated industries, such as financial services or healthcare, using shared or generic user IDs can violate compliance standards like SOX, GDPR, or HIPAA. Without proper tracking of who is performing specific actions, audits become nearly impossible, exposing organizations to legal and financial risks.

Further, in the event of a security breach or process failure, the lack of individual accountability makes it difficult to determine which bot or automated process was responsible. This delay in identifying the source of the problem can hinder effective incident response and prolong recovery time.

To address these challenges and minimize the risks of using service-type or generic user IDs for bots, organizations can adopt the following strategies:

STRATEGY	ADVANTAGE
IMPLEMENT ROLE-BASED ACCESS CONTROL (RBAC)	Ensure bots are assigned specific roles with the minimum required privileges to reduce the risk of unauthorized access.
ASSIGN AUTHORIZATIONS TO INDIVIDUAL USERS AND NOT THE BOT BASED IDS	BOTs can be shared, but not the IDs. BOT based IDs are usually shared and identifying and assigning the relevant authorization to the business user will have accountability, auditability, and security.
ENHANCE LOGGING AND AUDITING	Enable detailed logging of bot activities, including task execution times, data accessed, and changes made, to ensure transparency and facilitate compliance audits.
ADDITIONAL MONITORING	Utilize specialized tools to monitor bot performance, behaviour, and security, ensuring that any anomalies or security breaches can be detected in real-time.

Conclusion

Bots have the potential to greatly enhance SAP automation, but they also introduce security and compliance challenges, particularly when relying on service-type/generic user IDs for authentication. These IDs create risks related to traceability, accountability, and privilege management, which can undermine the benefits of automation. Organizations must adopt more secure identity management practices, such as individual bot IDs, robust auditing, and effective role-based access control, to mitigate these risks and ensure that automation efforts align with organizational security policies and regulatory requirements. By taking a proactive approach, enterprises can fully realize the advantages of SAP automation while safeguarding their systems and data.

Contact us for further inquiries

www.togglenow.com
sales@togglenow.com

TOGGLENOW®