Four Steps to Ensure Robotic Process Automation Security

By Naved Rashid, Associate Principal Analyst
Dionisio Zumerle, VP Analyst
Cathy Tornbohm, Distinguished VP Analyst

Gartner®

Four Steps to Ensure Robotic Process Automation Security

Published 15 January 2021 - ID G00735800 - 12 min read

By Analysts Naved Rashid, Dionisio Zumerle, Cathy Tornbohm

Initiatives: Security of Applications and Data; Identity and Access Management and Fraud Detection; Software Engineering Technologies

Enterprises are automating tasks with RPA, which creates security and noncompliance risks. Security and risk management leaders must ensure accountability for bot actions, avoid abuse from breaks in SoD, protect log integrity and enable secure RPA development to prevent unplanned business exposures.

Additional Perspectives

- Summary Translation: Four Steps to Ensure Robotic Process Automation Security (04 February 2021)

Overview

Key Findings

- Security is seldom the focus of RPA projects, especially with citizen developers creating RPA scripts, which results in a higher probability of security exposures such as data leakage and fraud.
- Even the most careful RPA design will generate privileged accounts and possible breaks in segregation of duties (SoD), which could lead to significant risks.
- Security and risk management leaders are concerned that RPA projects often overlook the security and audit capabilities of RPA tools, which exposes them to multiple vulnerabilities, such as storing sensitive client and/or supplier data in local systems.
- Security review of scripts is difficult to automate because of the nature of the scripts, and could prove to be a bottleneck in RPA implementation and change control process as the volume of bots increases.

Recommendations

Security and risk management leaders responsible for protecting enterprise applications and data must:

- Ensure accountability for bot actions and protect access to bots by assigning a unique identity to each RPA bot and process.
- Avoid abuse and fraud from breaks in segregation of duties by minimizing bot permissions and logging all bot interactions and user and transaction monitoring.
- Protect log integrity and ensure nonrepudiation by choosing a platform or tool that provides a complete, system-generated and immutable audit trail.
- Enable secure RPA development by implementing review and change control for RPA scripts.

Introduction

Business leaders are attracted to RPA technology (see Note 1), which can be quickly deployed to automate repetitive tasks, saving time and money for enterprises (for example, in contact centers or accounting departments). [1] RPA involves two main risks — data leakage and fraud — and proper governance, including security, is essential to mitigating these risks. RPA tools handle sensitive enterprise data, such as, copying and pasting account numbers and amounts from invoices to payment systems.

Without proper security measures in place, the sensitive data, such as RPA bot credentials or customer data that RPA handles, can be exposed to attackers and, especially, insiders. Furthermore, insiders can take advantage of the RPA access rights to insert fraudulent actions into the RPA scripts. Although RPA misimplementations can also lead to enterprise data corruption, this risk falls under the scope of resilience and is not addressed in this report.

As Figure 1 highlights, to address security failures in RPA projects, security and risk management leaders must:

- Ensure accountability for bot actions
- Avoid abuse and fraud from breaks in segregation of duties
- Protect log integrity and ensure nonrepudiation (see Note 2)
- Enable secure RPA development

Figure 1: Four Steps to Ensure Robotic Process Automation Security

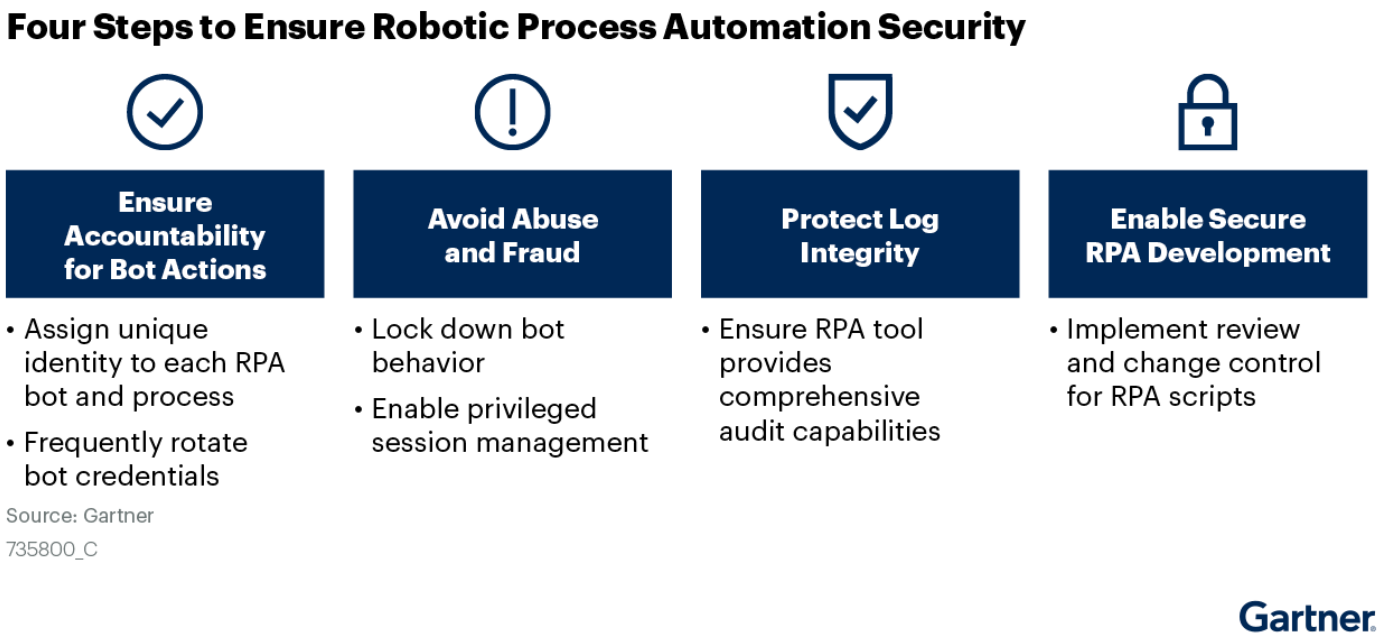
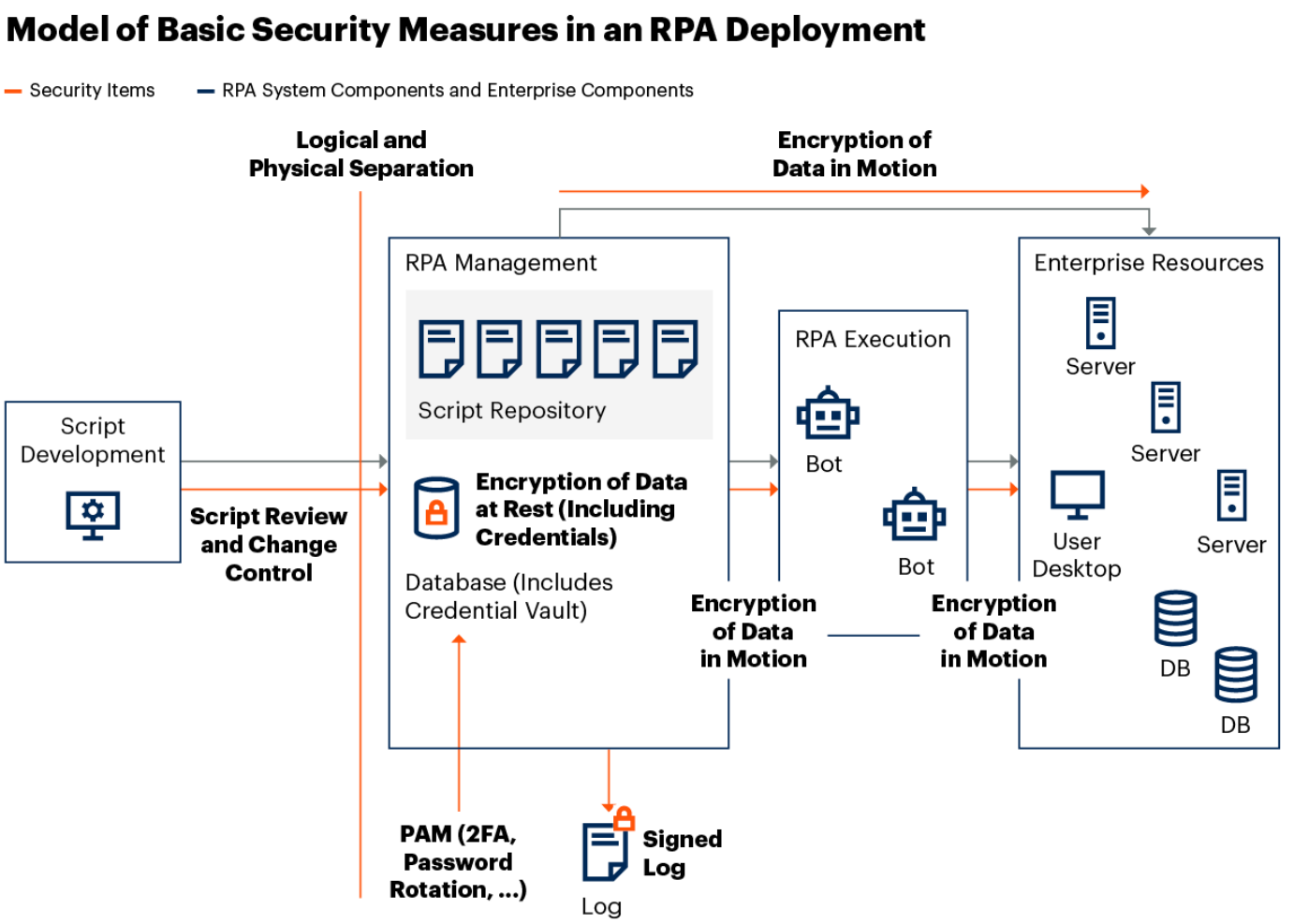


Figure 2 provides an overview of the areas where security leaders should intervene during RPA deployment and operations. Some areas that are obvious to security professionals, such as encryption of data at rest or in motion, are not dealt with in detail in this research. Rather, it focuses on the unique risks and security concerns introduced by RPA.

Figure 2: Model of Basic Security Measures in an RPA Deployment



Analysis

Ensure Accountability for Bot Actions

Bot operators are employees responsible for launching RPA scripts and dealing with exceptions. Sometimes, in the rush to deploy RPA and see immediate results, enterprises will not distinguish between the bot operators and the bot identities. The bots are run using human operator credentials.

This configuration makes it unclear when a bot conducted a scripted operation versus when a human operator took an action. It becomes impossible to unequivocally attribute actions, mistakes and, most importantly, attacks or fraudulent actions.

Another common bad practice is a bot identity created with powerful rights and then shared among different bots. The idea behind this is that the bot identity can be reused between different processes, and must therefore have powerful access rights (i.e., “it should be able to do anything”). This increases the risk of abuse and violates the principle of least privilege.

Using human operator credentials with bots also prevents increasing passcode complexity and frequency of rotation. These have to be limited to what is reasonable human user experience, rather than what a bot can handle. This eases brute force attacks and consequent data leakages.

- **Assign a unique identity to each RPA bot and process:** Bots should have dedicated identification credentials whenever possible. Identity naming standards should also distinguish between human and bot identities wherever possible. Use proper identity life cycle management for bot identities, assigning responsibility (but not the right to use those accounts!) to a group of users. This allows you to track who may be responsible for scripts that use a robotic identity. Also ensure that bot identities that are no longer required are removed. This can be done by looking at when they were last used and then consulting with the group responsible for the bot identity.

One example could be assigning B-123-X as an identity for the bot 123 operating a task called X. In addition, audit trails (logs) should provide the information that "a particular user asked bot B-123 to carry out task X."

An exception to this rule is constituted by "attended RPA" (such as call center operations) where human users leverage robotic automation technology on their computer to automate specific operations that are part of larger manual processes. This use case is also also called robotic desktop automation (RDA). In those cases, it is difficult to avoid reusing user credentials.

- **Use multifactor authentication for human access to RPA:** Rotate credentials for RPA bot accounts on an automatic and frequent basis (for example, using PAM tools). In RPA, two-factor human-to-system authentication is often considered simply using a device-bound certificate in addition to a username and password authentication challenge. Companies that have implemented RPA refresh bot passcodes frequently; some do so daily. Enterprises should take advantage of the fact that the user experience impact, which is often the main inhibitor for passcode rotation, does not apply in this context.

Although this can be achieved with existing enterprise infrastructure, privileged access management (PAM) tools can ease this process because they handle multifactor authentication, passcode rotation and automatic generation of credentials (see Magic Quadrant for Privileged Access Management).

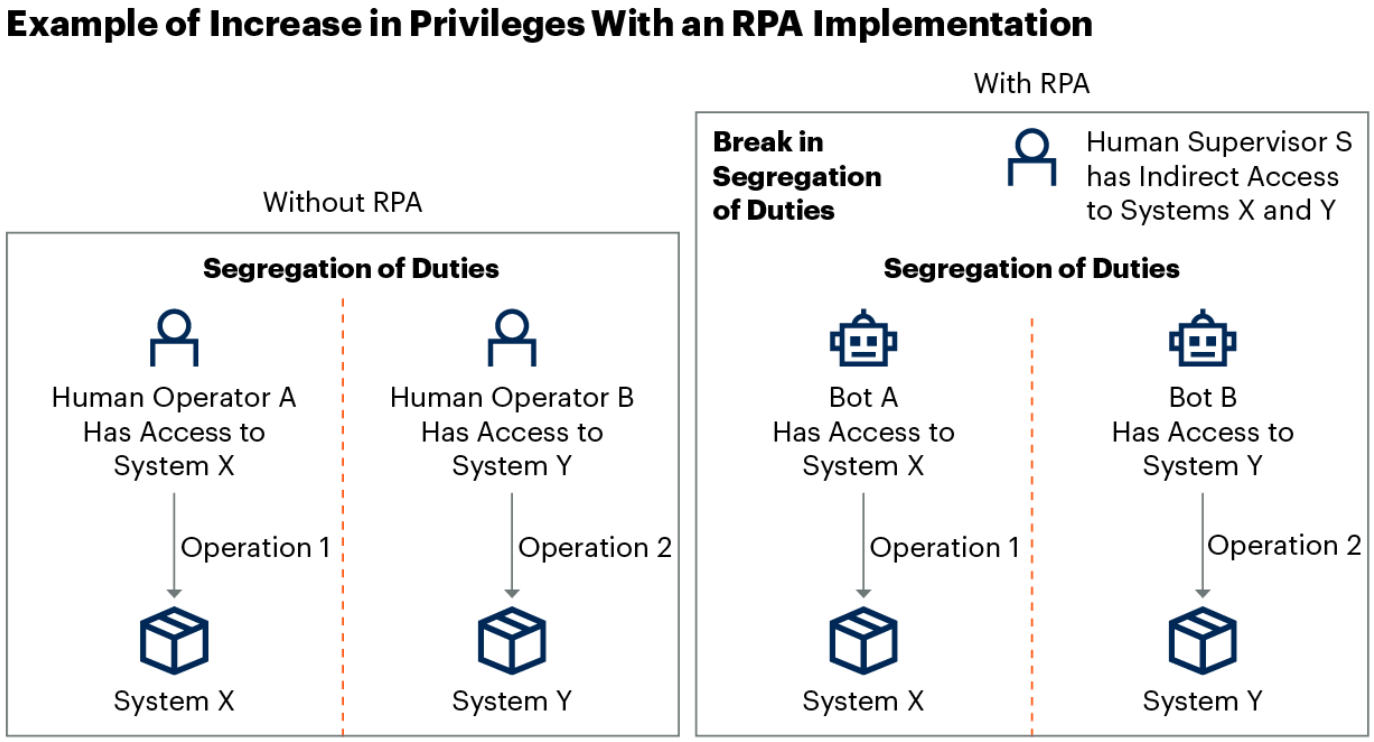
- **Do not hard-code credentials in RPA scripts:** RPA scripts leverage enterprise credentials for bots to perform actions on enterprise systems. Some enterprise systems directly integrate with directory services, and the RPA script can retrieve credentials from the directory. For other systems, these credentials should be stored in a hardware security module, if the enterprise has one, or the RPA credential vault.

Alternatively, if the organization has PAM in place, application-to-application password management (AAPM) capabilities of the PAM tool can be used. Certain PAM and other tools can assist with automated checking for hard-coding in scripts. The RPA credential vault is essentially a protected database that encrypts credentials. Each time the RPA script requires using credentials, it should reach out to the directory or the vault, where the credentials should be stored cryptographically protected. PAM tools can integrate with the RPA vault for rotating and updating bot credentials.

Avoid Abuse and Fraud From Breaks in Segregation of Duties

Even the most careful implementation of RPA can lead to an increase in account privileges, thereby increasing the risk of fraud. Take, for example, an organization where two human operators, A and B, have access to Systems X and Y, respectively. If the tasks of operators A and B are replaced by an RPA tool, then the RPA bot has to have access to both Systems X and Y. Ignoring any licensing impact, creating two separate bots with separate credentials and entitlements can mitigate the issue. However, the segregation of duties problem still persists with the human operator that oversees the RPA operations for both bots, especially in the attended automation use case. Alternatively, putting in place two human operators — one to oversee each bot — takes away the advantage of automation. Figure 3 illustrates the issue.

Figure 3: Example of Increase in Privileges With an RPA Implementation



Source: Gartner
735800_C

An example of how this increase in privileges can lead to fraud can be a supervisor responsible for payment processes creating a fake provider account and scheduling related payments to this account. Because the operation is conducted by a bot, it is less likely to be detected.

- **Separate developers and bot operators:** Segregation of duties has to take place between developers of RPA scripts and human operators of bots. To mitigate fraud risks, RPA script developers should not be able to run the bots on production systems. Conversely, human supervisors of bot operations should not be able to define and develop RPA scripts. Some of the clients that Gartner has talked to not only protect the logical access to bot operations, but also physically separate the location where bots are executed.

- **Enable session recording for interactive access when bot accounts are used:** Session management should include either screenshot or video monitoring to dissuade fraudsters and conduct forensic investigations. Bot credentials should always be hidden from administrators, and any disclosure should be explicit (i.e., requiring approval), short-term and scrutinized.

- **Ensure close monitoring and fraud management, especially where breaks in segregation of duties are unavoidable:** Manual processes are often used today to decrease the risk of fraud with RPA. Organizations identify points in their automated processes that are susceptible to fraud and ensure that there is independent review of all related transactions. In these cases, the maker-checker principle (or the four-eyes principle) is also used for authorization. Certain RPA tools (as well as some PAM tools) provide this feature. For example, for transactions over a certain threshold, with RPA tools, one bot makes the operation, and another bot verifies the correctness of the operation and approves it. The exact implementation can vary. In certain RPA implementations, Gartner observed that a human performs the verification.

- **Implement PAM when making use of RPA:** PAM will speed up and structure the processes described above, even though only a minority of end-user organizations are currently leveraging PAM integrated with RPA. Magic Quadrant for Privileged Access Management contains a list of options and vendors, some of which already have integrations with RPA vendors.

- **Lock down bots:** Unlike human operator behavior, bot behavior is predictable. Locking down bot access and privileges does not result in complaints about user experience, as it would from a human user. Security leaders should restrict RPA access to what each bot strictly needs to conduct the assigned task. For example, an RPA script with a bot that copies certain values from a database and pastes them into an email should only have read access to the database, rather than write access.

- **Most RPA tools provide role-based and resource-based access controls to restrict access to RPA functionality:** RPA tools can also integrate with enterprise directory services, which can help restrict access to enterprise resources and assign account privileges correctly. Some organizations have expressed concerns about allowing RPA to modify databases directly. This could lead to data tampering, but most importantly to data corruption, which we do not focus on in this research. Alternatively, tools such as database activity monitoring in front of the databases will provide monitoring.

Protect Log Integrity and Ensure Nonrepudiation and Compliance

Whenever there is an RPA security failure, the security team will need to review logs. A log, or audit trail, of RPA activity is paramount to ensuring nonrepudiation and to enable an investigation when needed.

RPA tools provide logging of the actions a bot has taken in the applications it has accessed.

In addition to PAM, tools that provide insider threat detection, such as Ekran System or ObserveIT, can record sessions to show who accessed an account and what interactive actions were made. Enterprises typically feed RPA logging to a separate system where the logs are stored securely and are forensically sound, such as a central log management or SIEM tool (see Magic Quadrant for Security Information and Event Management).

- **Ensure that the RPA tool provides a complete, system-generated and immutable log of its activity:** The log must be complete, as gaps would hinder any investigation or make the security team miss important alerts. It should also be integrity-protected to ensure it is immutable; one way to do so is by signing the log. To ensure script integrity, the log should also take into account changes made to scripts by developers or other parties.

- **Require an assessment of the RPA tool from a testing vendor:** RPA tools often provide assurance that they have been tested for vulnerabilities from an application security testing vendor. This assessment report should be required because nonremediated vulnerabilities can be leveraged by attackers.

Enable a Secure RPA Development

Many RPA initiatives are led by the line of business. Security leaders are consulted sporadically, if at all, during development. Establishing early on a common language and a dialogue between the security team and the line-of-business team that leads the RPA initiative is essential. This may entail establishing a risk framework, whereby the RPA implementation as a whole, as well as the individual scripts, are evaluated in terms of risk (see Cyber Judgment: Navigating the Era of Distributed Risk Decision Making).

To speed up deployment, enterprises tend to postpone security considerations until RPA scripts are ready to run. This approach allows security flaws not simply in scripts, but also in the entire approach to RPA, to go undetected until it is too late. As RPA usage increases, manual script review can become overwhelming. Recently Gartner has started observing RPA vendors and application security testing vendors that offer RPA script reviews [2] and RPA security assessments.

- **Implement change control for scripts:** Periodically review and test RPA scripts with a special focus on business logic vulnerabilities. In most cases, this review will take place in a peer review fashion, whenever there is change in the script. Some application security and penetration testing vendors are starting to offer assessments as well.

- **Use caution when utilizing free versions of RPA tools with sensitive data:** Often, free versions of RPA tools are intended only for trials and do not provide security functionality.

Evidence

[1] When and Where to Use Robotic Process Automation in Finance and Accounting

[2] "Industry First Bot Security Program,"

Note 1: Robotic Process Automation

Robotic process automation (RPA) typically uses a combination of user interface (UI) interactions and APIs to integrate and perform data transcription work between different enterprise and productivity applications. RPA automates repetitive human tasks by emulating the same human transaction steps, mainly via orchestrated UI interactions.

Note 2: Nonrepudiation

In information security, nonrepudiation is the property of being able to confirm the identity of a specific party, or the action conducted by it. In the context of asymmetric cryptography, for example, a party that signs a message with its private key guarantees, when sending that message, that the content has not been modified and that it is the originator of that message.

Document Revision History

Top Four Security Failures in Robotic Process Automation - 9 February 2018

Recommended by the Authors

Critical Capabilities for Robotic Process Automation

Magic Quadrant for Robotic Process Automation

Follow these best practices to create a resilient, scalable and agile cybersecurity strategy.

The IT Roadmap for Cybersecurity

About Gartner

Gartner is the world's leading research and advisory company and a member of the S&P 500. We equip business leaders with indispensable insights, advice and tools to achieve their mission-critical priorities today and build the successful organizations of tomorrow.

Our unmatched combination of expert-led, practitioner-sourced and data-driven research steers clients toward the right decisions on the issues that matter most. We are a trusted advisor and an objective resource for more than 14,000 enterprises in more than 100 countries — across all major functions, in every industry and enterprise size.

To learn more about how we help decision makers fuel the future of business, visit gartner.com.

Become a Client

Get access to this level of insight all year long — plus contextualized support for your strategic priorities — by becoming a client.

gartner.com/en/become-a-client

U.S.: 1 800 213 4848

International: +44 (0) 3331 306 809

Gartner®