



# **RPA Security**

All technologies have security vulnerabilities that can be exploited by bad actors. Luckily, new technologies have well-established and battle-tested mitigation plans for their known security risks, enabling developers to detect security vulnerabilities at all levels of the technology stack. Empowered by these insights, technology leaders can create and deploy security mitigation plans to reduce and eliminate these risks.

With Robotic Process Automation (RPA), common security concerns focus on human user access management, bot privileges, data security, and meeting security regulation requirements. The three leading RPA software providers, UiPath, Blue Prism, and Automation Anywhere, offer many native security features and the ability to integrate with more robust security tools. Developers guiding clients through “first steps” of RPA must ensure necessary software approvals and accompanying workflow systems are obtained and maintained. From advising on the integration in the broader security landscape to employing best practices in development and testing, technology leaders should work with stakeholders across every step of their automation journeys to provide them with confidence that they have the highest appropriate level of automation security.

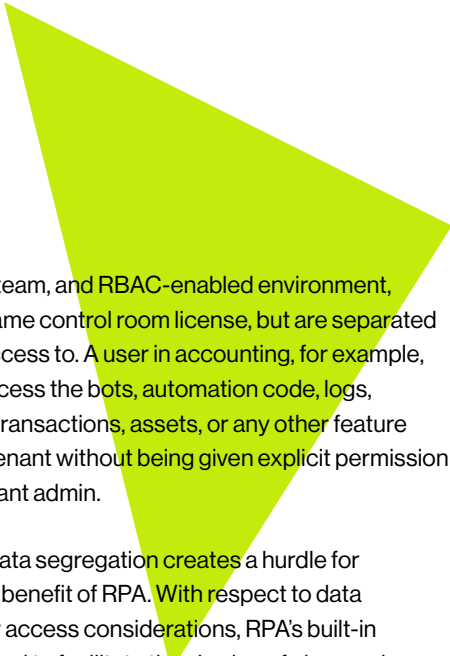
---

## RPA Security Considerations

### User Access Management

One of the primary benefits of RPA is the central management of automations and their related data, but that also introduces security risks. With all automations and associated credentials, logs, monitoring data, and other information in one location, it is essential to follow best practices to ensure users only have access and authorization to the data they need. By contextualizing the native features of RPA tools with these priorities, organizations can ensure they have a secure foundation throughout their automation journey.

The leading RPA providers include built-in features to enable a security design that responds to user access management considerations. Employing segregation of duties and the principle of least privilege, users have the lowest level of access required to complete their job. Automation Anywhere offers configurable Role-Based Access Control (RBAC) tools to manage dynamic user access needs efficiently. UiPath promotes “tenancy” in their control room (Orchestrator), allowing them to divide the control room into business unit tenants. Blue Prism also offers an architecture similar to UiPath with their Multi-Team Environments.



In a multi-tenant, multi-team, and RBAC-enabled environment, users operate on the same control room license, but are separated in the data they have access to. A user in accounting, for example, would not be able to access the bots, automation code, logs, schedules, audit trails, transactions, assets, or any other feature from the supply chain tenant without being given explicit permission by the supply chain tenant admin.

The security need for data segregation creates a hurdle for reusability — a primary benefit of RPA. With respect to data confidentiality and user access considerations, RPA's built-in features can be leveraged to facilitate the sharing of cleansed workflows and other data artifacts, promoting automation development efficiency via reusability.

### Bot Privileges

Security risks around bot access are different from those around human user access. RPA bots do not have the autonomy to act with malicious intent unless they are programmed to do so. The actual risks around bot access are rooted in accountability.

Reactive measures for bot accountability include traceability, meaning the ability to trace which actions the bot performed and when it performed them. To ensure full traceability of bot actions, each bot needs to be uniquely credentialed and identifiable. Proactive methods for accountability include limiting the bot's access via RBAC and attribute-based access control. Whenever modifications are made to the automation code, it is imperative to revisit the implemented security measures as the new code may introduce new security vulnerabilities to the system.

Organizations should support RPA developers in maintaining best practices around bot password management, such as creating randomized passwords that are updated at specified time intervals. Categorizing bots by security level provides clarity and control around the appropriate frequency for password update process. It is also important to note, **plaintext passwords should never be stored in automation code**. There are multiple strategies for RPA bot password management, including:

- Native RPA software password vaults (e.g., storing credentials in UiPath Orchestrator as “assets”).
- Windows Credential Manager.
- Integrating with more robust Password Access Management (PAM) tools.

The agency or firm implementing RPA may have existing enterprise PAM tools, such as CyberArk, used to manage credentials. These tools deliver in-depth-defense security by managing and protecting privileged credentials, used by both human (passwords and Secure Shell (SSH) keys) and non-human users (hardcoded application credentials). Integrating RPA software with PAM systems enables users to store credentials securely within password vaults and allows the robots to retrieve the required credentials through the control room, performing automations in a secure manner.

## Data Security

Firms with access to classified, sensitive, and private data should prioritize data security across all of their endeavors, embedding security training as part of their DNA. Paired with expert knowledge of each of the major RPA vendors' security features, technology leaders can promote current best practices through the entire automation life cycle, ensuring that data security is maintained with colleagues and clients alike.

There are several data security features available in RPA software. A couple of the most valuable and commonly used are:

### Input Lock

In cases where users have view but not edit access, Automation Anywhere's "input lock" feature is most appropriate. This feature disables the mouse and keyboard for the machine on which an automation is running.

### Obfuscation

Other processes may benefit from more secure data protection by preventing even the display of sensitive data. For these cases, Blue Prism promotes obfuscation techniques, including:

**Cipher obfuscation:** Encrypts credential information. This technique reduces the risk of unauthorized data access.

**Simple obfuscation:** Encrypts information that is serialized/deserialized across boundaries. This technique serves as an additional level of encoding, offering additional protection against interception and deciphering of data by bad actors.

**Source-code obfuscation:** Encrypts source-code in its majority using an industry-leading obfuscation tool. This technique reduces the risk of successful reverse engineering and malicious patching by increasing the task's complexity and the time needed to decipher it.

Automation Anywhere also offers a "stealth mode" feature, which prevents all working programs from being displayed. Additionally, users can disable image capture on Bot Creators and Bot Runners, thereby preventing sensitive information displayed on screen from being stored in the automation code. Similarly, in UiPath, users can check the "hidden" property on activities that engage sensitive applications or data.

Beyond the data security tools available in RPA software, standard encryption is also applied to data at all processing stages:

### Data at Rest

- Federal Information Processing Standards (FIPS)-compliant options

### Data in Use

- Microsoft's SecureString functionality, built into the .Net framework

### Data in Motion

- Transmission Control Protocol (TCP), Windows Communication Foundation (WCF), and Hypertext Transfer Protocol (HTTP)-based communications
- Transport Layer Security (TLS) 1.2 enforced for TCP and HTTP protocols
- Advanced Encryption Standard (AES) 256-bit encryption



## Security Regulation Requirements

To support the detailed logging of bot information, RPA software providers also offer frameworks with built-in logging capabilities, which standardize logging and add efficiency to the development process.

Below is a summary table of common security standards and regulations, with which the three leading vendors are compliant and/or enable as of September 2020.

Security Standards and Regulations	UiPath	Blue Prism	Automation Anywhere
ISO27001:2013 certified	✓	✓	✓
VERACODE “Verified Continuous”	✓	✓	✓
General Data Protection Regulation-compliant	✓		✓
Federal Information Processing Standards (FIPS)		✓	✓
Payment Card Industry Data Security Standards (PCI-DSS)		✓	✓
Health Insurance Portability and Accountability Act (HIPAA)	✓	✓	
Sarbanes-Oxley Act (SOX)		✓	
Federal Information Security Management Act (FISMA)	✓		✓

When developing RPA strategy, technology leaders must build a foundation of security to ensure solution durability and reliability. The baseline tenets of automation security include managing human user access management, bot privileges, and data security, but ultimately, RPA must meet all pertinent security regulation requirements. By understanding these considerations, technology leaders can provide stakeholders with confidence that their systems, data, and processes are secure throughout the entire automation lifecycle.

For more information, please contact:

### Shelby Pons

Senior Consultant, Advanced Analytics and Intelligent Automation  
spons@guidehouse.com

## About Guidehouse

Guidehouse is a leading global provider of consulting services to the public and commercial markets with broad capabilities in management, technology, and risk consulting. We help clients address their toughest challenges with a focus on markets and clients facing transformational change, technology-driven innovation and significant regulatory pressure. Across a range of advisory, consulting, outsourcing, and technology/analytics services, we help clients create scalable, innovative solutions that prepare them for future growth and success. Guidehouse is a Veritas Capital portfolio company, led by seasoned professionals with proven and diverse expertise in traditional and emerging technologies, markets and agenda-setting issues driving national and global economies. For more information, please visit: [www.guidehouse.com](http://www.guidehouse.com).