AUTOMATION ANYWHERE

Enterprise-class Security for Robotic Process Automation

INTRODUCTION

Why, after 20+ years of investment in business process automation technologies, less than 20% of the tasks have been automated? The primary reason is the lack of well defined APIs in 85% of the enterprise systems. The result is an ever growing IT backlog of integration requests from line of business.

Robotic Process Automation was born with the vision of empowering business users to create software bots that could interact with enterprise systems just like humans. RPA bots can log into enterprise applications using credentials, just like humans, and automate tasks that involve any enterprise application, including legacy applications without APIs. Claims processing, loan processing, account reconciliation, invoice generation/submission, and report generation are just a few examples of potential automations that span across different business disciplines.

It is easy to see the potential for substantial time and cost savings, improved customer satisfaction, increased workforce morale, and the ability to build a commanding advantage over competitors using RPA. Fully realizing these gains depends, however, on having an enterprise-class solution.

Providing rock-solid reliability, scalability, and an extensive feature set for maximizing applicability and usability are some of the essential criteria for automation. But these elements are not covering the business' most critical requirement: end-to-end security. A robust security architecture with features that enable full support for core principles, such as least privileges and separation of duties while delivering end-to-end protection for the critical apps and sensitive data involved, are mission critical.

This paper provides an overview of the industry's highest standard for enterprise-grade security as demonstrated by the market's leading Digital Workforce platform, Automation Anywhere Enterprise.

“

It is easy to see the potential for substantial time and cost savings, improved customer satisfaction, increased workforce morale, and the ability to build a commanding advantage over competitors using RPA. Fully realizing these gains depends, however, on having an enterprise-class solution.

ARCHITECTURE AND OPERATIONS

Understanding the security controls needed for an enterprise-class RPA implementation depends on the understanding of the components that comprise the solution and their operations.

Core Components

As shown in **Figure 1**, the core building blocks of Automation Anywhere Enterprise are the Control Room, Bot Creators, and Bot Runners.

Control Room

Control Room serves as the brain of the automation environment. It is a Windows server-based management system, with an integral database, that provides a unified view for the overall system administration. Control Room is also where RPA operators go to orchestrate the Digital Workforce—in other words, to schedule, deploy, execute, monitor, and manage the operation of the organization's bots. In addition, built-in version control features (Apache Subversion Server) facilitate multi-user collaboration while enforcing change management best practices and establishing a centralized repository of production-ready bots.

Bot Creator

Bot Creator is used to build bots. It is a Windows desktop app running on a workstation class or virtual machine, the Bot Creator is used by business process experts to create and test their automations. Bots are created utilizing the Bot Editor, while bot testing – using local, non-production test data and app instances – is facilitated by the Bot Runner. Following successful testing (e.g., for performance, data integrity, and security), bots are checked into the Control Room repository and become available for production deployment.

Bot Runner

Bot Runner puts bots to work. Using the same application code as the Bot Creator, but with a different license key, the Bot Runner executes bots in the production environment – that is, utilizing production instances of the target application and production data stores. In fact, running bots is all Bot Runners can do, as creation and editing functions are not available to them. For highly reliable, large-scale operations, pooling of Bot Runners is also supported.

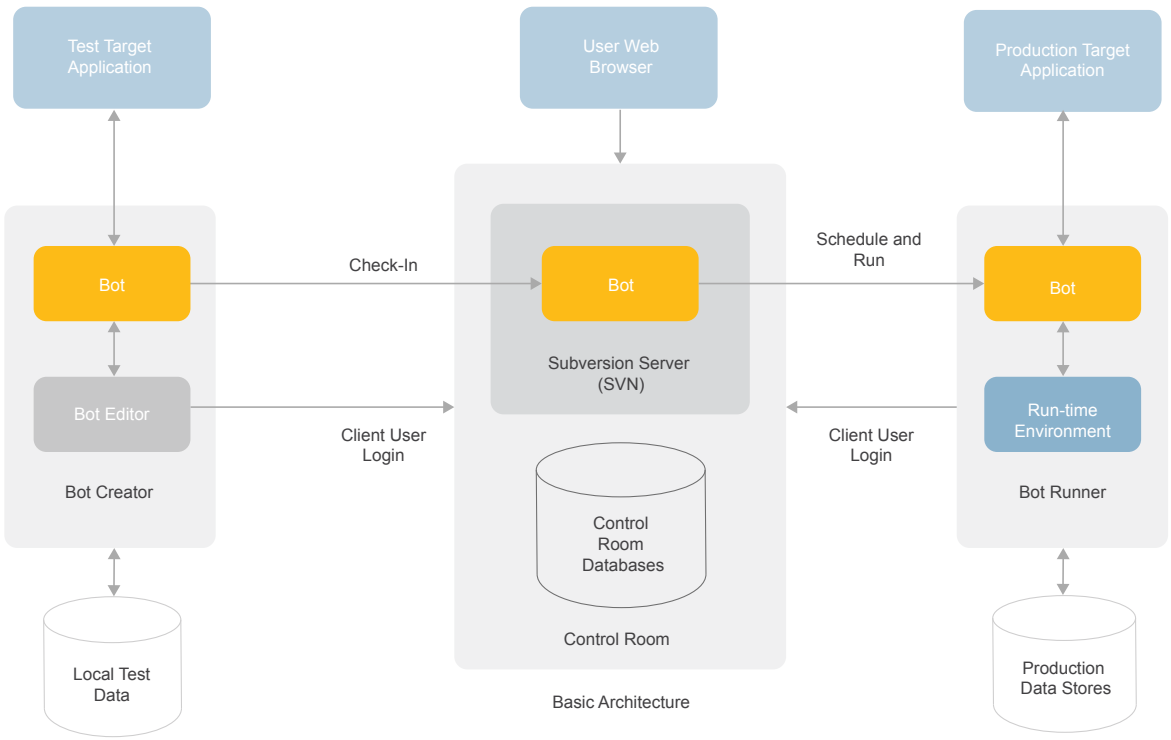

Figure 1: Basic Automation Anywhere Enterprise Architecture

Additional Enterprise-class Components

When considering large-scale operations, two other important RPA solutions relevant to organizations pursuing enterprise-grade deployments emerge: on-demand scaling and Bot Insight.

On-demand Scaling

Leveraging Amazon Web Services (AWS) public cloud, Automation Anywhere Enterprise effectively delivers RPA-as-a-service, with all the attendant capabilities – including elastic ramp-up/ramp-down, usage-based metering, unlimited horizontal scalability, and continuous monitoring and audit-logging of Bot Runner infrastructure. The result is multi-node high availability that powers SLA-driven performance and business continuity, even when there are dramatic swings in automation workload.

Bot Insight

A fully integrated subsystem within the Control Room, Bot Insight performs near real-time analysis of bot operations and business process data. Bot Insight automatically generates customizable dashboards using advanced algorithms unique to each bot. The level of detail Bot Insight provides based on fine-grained event logs on bot operations, permits nuanced alerting, ad-hoc discovery, interactive drilldowns, time-series analysis and comprehensive insight into operational/business processes. In addition, all data can be exported for Security Information and Event Management (SIEM) logs for further analysis, investigation, and reporting.

Bots in Action: Two Types of Automations

One final thing to clarify before launching into Automation Anywhere Enterprise's high-grade security capabilities are the two basic types of automations: attended and unattended.

An attended automation is one where a user is logged in on the Bot Runner machine to observe and/or actively support bot execution. Reasons for having a user present may be that the bot serves a utility type function that aids in their work, or that the bot performs batch-type work that requires periodic input or situational direction from a user. Attended automations are also referred to as front-office automations.

Unattended automations, as their name suggests, operate without any need for business user or operator interaction. Unattended automations are typically run by an operator who has little knowledge about the bot, the application being automated, or the purpose of the automation. The operator, in conjunction with the business unit, schedules bots to run on Bot Runners. During execution, the operator monitors operational aspects of the running bots, such as CPU, memory, and storage usage to ensure they execute without any errors or exceptions. Control Room dashboards display all operational details of the bots as they are running. If an unattended automation does not complete due to an error, the operator might implement procedures to fix the automation and restart it; otherwise, they will escalate to the RPA team or business unit to diagnose and fix the issue.

MULTI-LAYER ENTERPRISE RPA SECURITY MULTI-LAYER IDENTIFICATION AND AUTHENTICATION

A core tenet of the Automation Anywhere Enterprise's security architecture is that no access or action is permitted without prior authentication of the involved entity. This applies to humans and bots alike. The result is a multi-layer authentication process for both attended and unattended automations.

WHO'S WHO: TYPICAL ENTERPRISE AUTHENTICATIONS

Credentials and Personas can be multi-layered. Consider a simple enterprise authentication scenario (see **Figure 2**). An enterprise user, Alice, authenticates to her Windows workstation. Alice then logs in to an application that is running remotely, authenticating via a Windows Domain Active Directory login or perhaps Kerberos based on her workstation having a valid ticket. In this scenario, the chain of authentication involves a single person and their credentials.

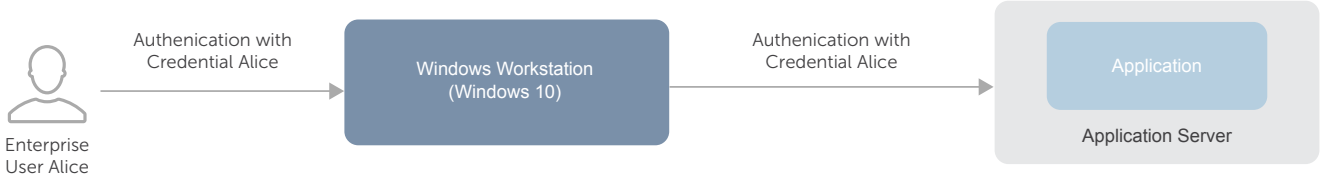

Figure 2: Typical Enterprise Authentication

Now consider the attended automation scenario shown in **Figure 3**. In this case the user, Bob, is either testing a bot or running an attended automation as part of his typical work day. In step 1, he authenticates to the Bot Runner workstation using his personal credentials (just like in the Alice scenario above). In step 2, he launches the Automation Anywhere Enterprise client and enters his Control Room user ID and password, thereby authenticating the client software to the Control Room. In step 3, he runs the bot which, in turn, accesses an application that requires authentication. The credentials used by the bot at this step can either be stored in the Enterprise Credential Vault and retrieved by the bot during runtime, or there can be a pass-through of Bob's personal credential (based on clearance afforded by his workstation and the application server being in the same domain). Either way, the result is three layers of identification and authentication in total.

There are three layers of authentication used for the unattended scenario depicted in **Figure 4**—albeit with a couple of twists. In this case the user, Charles, starts by authenticating to the Control Room so that he can select a bot to run, either immediately or at a scheduled time.

In step 2, when the time for bot execution begins, the Control Room initiates an auto-login to the Bot Runner workstation, using the BotRunnerUser credential. After the bot is downloaded to the local Player function (step 3) and starts to execute, it authenticates to the target application using the BotApplicationUser credential (step 4). Just like the attended automation scenario, the BotApplicationUser credential may be one that is retrieved from the Credential Vault, or it may be a pass-through of the BotRunnerUser credential.

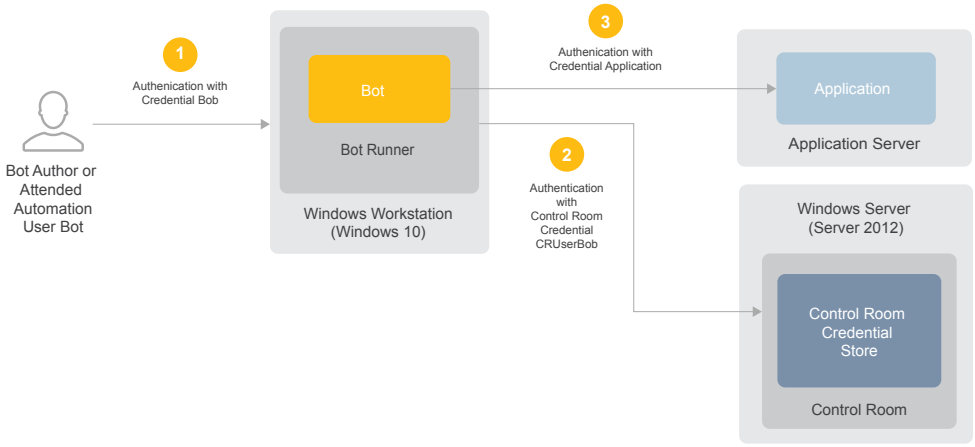

Figure 3: Authentication Process for Attended Automation Scenario

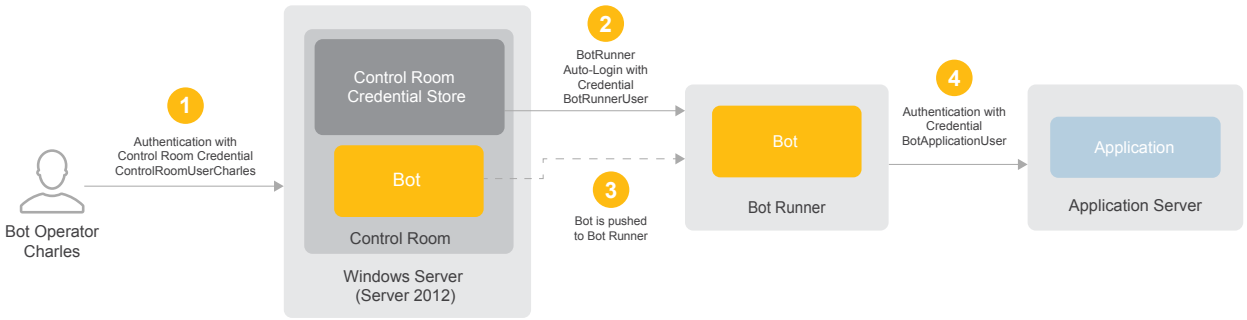

Figure 4: Authentication Process for Unattended Automation Scenario

Authentication Options and IAM Integrations

Supported options for Control Room authentication include Active Directory using LDAP, Active Directory using Kerberos, and local authentication using the embedded Credential Vault (discussed in a later section).

Other identity and access management options available for enterprise deployments, include:

+ Support for SAML 2.0 based single sign-on
+ Integration with 3rd-party privileged access/credential management solutions (e.g., CyberArk, One Identity, and Thycotic)

COMPREHENSIVE ROLE BASED ACCESS CONTROL

Successful authentication is only the first level of mandatory access control enforcement afforded by the Automation Anywhere Enterprise security architecture. Equally important, especially when it comes to adhering to the core principles of least privileges and separation of duties, is support for fine-grained Role Based Access Control, or RBAC.

There are five distinct roles (see **Table 1**) to consider within the basic architecture and primary functions of the RPA platform. BotBuilders utilize the Bot Creator to capture business logic and create corresponding automations. BotBuilders work with test applications and data sets so that production systems are not impacted during the development phase. An individual bot will typically go through many different iterations and versions, not only during initial development but also whenever the associated business processes and/or target application is updated. BotTesters also work with the Bot Creator to test bots for performance, data integrity, and security, making sure each bot does what it is intended to do in a secure way. BotTesters serve as a second stage of authorization for the bot before it can run with production data and applications.

Once a bot has been tested and has undergone a security review, the BotPromoter works with the BotBuilders/BotTester to designate the version of the bot that should be used in production. This is the only version of the bot that will be visible to the BotOperator, who coordinates with the business unit(s) to schedule and run the bot. The BotOperator is also responsible for the monitoring of bot performance within the Control Room, including troubleshooting any runtime problems that arise. Finally, responsibility for overall administration of the platform – including configuring components, interfaces, and all roles/permissions – falls on the RPA Admin.

Advanced Separation of Duties

This core set of roles demonstrates a basic starting point for RBAC, but even greater separation of duties is possible within the Automation Anywhere Enterprise platform. Using the embedded role creation wizard, administrators can easily define custom roles, setting privileges/permissions that account for the full suite of Control Room objects and functions, including user management, licensing, Credential Vault, sets of Bot Runners, bot schedules, bot operations/dashboards, and audit logs. As each privilege is selected, the wizard will dynamically add steps for contingent/derived privileges.

For example, when the BOTS > View my bots > Run My bots privileges are selected (see **Figure 5**), the workflow will add a step to indicate the specific Bot Folders (i.e., sets of bots) for which access is being granted. The net result is the ability to establish high-fidelity roles with fine-grained access controls sufficient to meet the needs of the most stringent, secure, and compliance-regulated environments.

Role	Description
RPA Admin	Administers the system (configuring components, roles, interfaces)
BotBuilder	A business process expert who creates bots with the Task Editor and performs basic functional testing
BotTester	A quality assurance tester that reviews the bots for functional accuracy, performance, and security
BotPromoter	An administrator that approves and moves bots between dev, test, and production stages
RPAOperator	An operator who schedules, runs, and monitors the performance of bots

Table 1: Primary RPA Roles in Automation Anywhere Enterprise

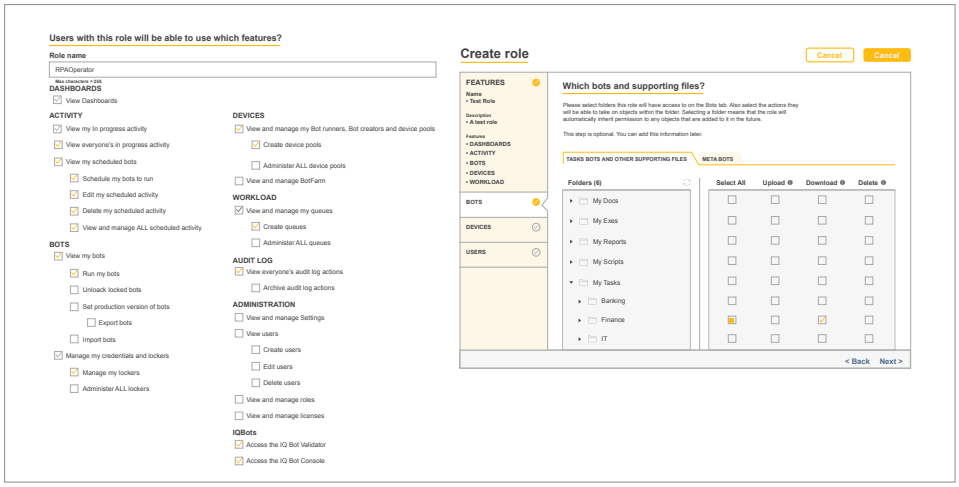

Figure 5: Role Creation with Fine-Grained Authorization

Independent Control Planes

Beyond extensive RBAC capabilities, Automation Anywhere Enterprise inherently delivers logical separation of duties by employing an architecture that thoroughly separates the tasks of bot development and bot execution.

Bot Creators can only upload and download bots to and from the version control system within the Control Room. At the same time, Bot Runners are limited to executing bots; they have no access to bot creation and test functionality. This architecturally enforced separation of duties constitutes a dual authorization consistent with National Institute of Standards and Technologies (NIST) best practices, as it requires (at a minimum) both a developer and business user to ultimately enable a business process automation.

Independent Processing Domains

A powerful use case for the platform's RBAC capabilities, especially for large enterprises, is the establishment of independent processing domains (see **Figure 6**). This can be accomplished by strictly organizing/storing the bots for each desired domain in a corresponding folder within the Control Room.

Case in point: Bots associated with finance applications would be placed in a finance folder, while those associated with HR would be placed in an HR folder. Bot operators for the finance department would then be assigned privileges solely for finance bots and finance Bot Runners; bot operators for HR would get privileges solely for HR bots and Bot Runners, and so forth for other processing/automation domains (see **Figure 6**).

The net result is further separation of duties and isolation of associated apps and data—this time at the OU/domain level—as individual operators are unable to see or operate bots outside of their given domain.

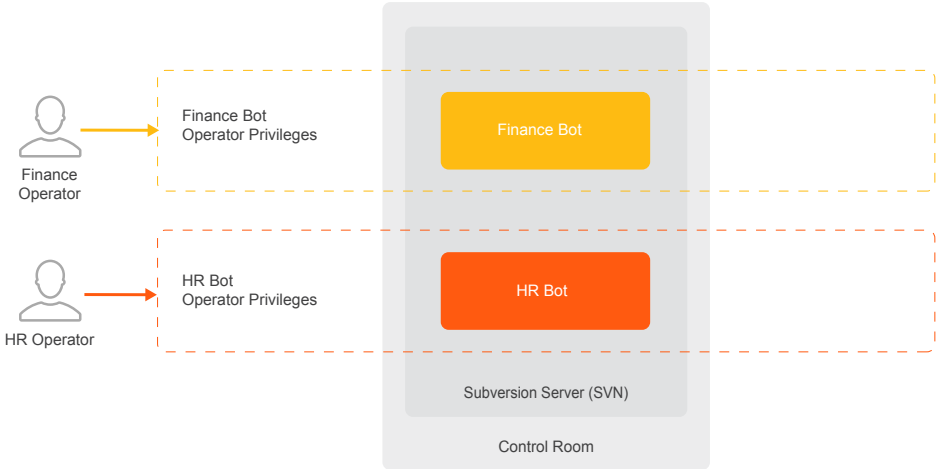

Figure 6: Support for Independent Processing Domains

END-TO-END DATA PROTECTION

Multi-layer authentication and fine-grained access control are essential for a tightly controlled environment. So is end-to-end data protection, which is also necessary to maintain the confidentiality and integrity of business-critical processes, sensitive data, and related secrets (e.g., credentials).

The Automation Anywhere Enterprise platform addresses this need with an embedded Credential Vault and provides an extensive set of safeguards that not only protect data at rest and in transit, but also while it is in use on individual systems.

Encryption Keys and the Credential Vault

Figure 7 shows the primary encryption keys used by the platform, along with their relationship to the Credential Vault. All encryption is performed using FIPS 140-2, Level 1 validated cryptographic modules.

During installation (left portion of **Figure 7**), the system generates an RSA 2048 bit public/private key pair and an AES 256 bit key. The private key of the RSA 2048 pair is referred to as the Master Key, while the AES 256 key is referred to as the Data Key. The Master Key is presented to the installing administrator for safekeeping in a physically secure location off system. The public key is used to encrypt the Data Key. Both the public key and the encrypted Data Key are then stored in the database. When in use, all keys and encrypted data are placed in encrypted secure memory using the Microsoft Data Protection API (DPAPI).

During Control Room startup or reboot (right portion of **Figure 7**), the administrator is prompted to supply the Master Key. The encrypted Data Key is retrieved from the database and decrypted using the Master Key. The Data Key is now ready for use. As the system stores and retrieves data from the Credential Vault, the Data Key is used to encrypt and decrypt that data.

The Credential Vault is used to store all system managed credentials and critical system configuration data. It can also be used to store any other sensitive data (e.g., name-value pairs) used in an organization's automations. As a result, BotBuilders can avoid the insecure practice of hard-coding credentials and other sensitive data/arguments directly within their automations.

Protection of Data at Rest

In addition to encrypting local credentials and selecting runtime data used by bots, the Credential Vault provides secure storage for sensitive configuration parameters and details pertaining to the integral version control and email services.

Protection of Data at Transit

All network services on the clients and the Control Room use Transport Layer Security (TLS) 1.2 to assure data security and integrity during transport between components.

Credentials used for Bot Creator/Runner authentication to the Control Room are encrypted prior to being submitted over a TLS-secured connection. This extra layer of encryption not only protects against network stack issues (such as Heartbleed), but also prevents exposure of the credentials for implementations where the outer-layer TLS connection is terminated at a front-end load balancer.

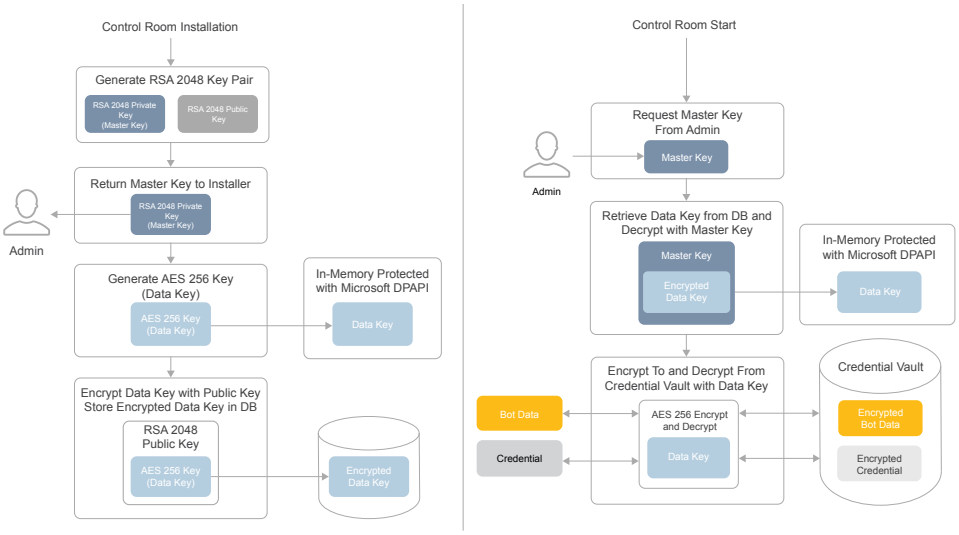

Figure 7: The Automation Anywhere Enterprise Encryption Architecture

Protection of Data in Use

Runtime security begins with distributed credential protection. Specifically, there is no local credential storage on Bot Runners. Credentials and other data dynamically retrieved from the Credential Vault for use within automations is retained solely in encrypted format in volatile memory – and gets wiped once the associated bot is finished executing.

Other features and configuration options that can be used to prevent unauthorized access to confidential information (i.e., data leakage) or tampering with bots during runtime include:

+ Stealth mode – where no program windows are displayed on the local screen and logged in users have the option to disable image capture on Bot Creators and Bot Runners, thereby preventing sensitive information displayed on-screen from being stored in bots
+ Input lock – the ability to disable the mouse and keyboard for the machine where an automation is running
+ Time limit – the ability to set a time limit after which an automation will be terminated if it has not finished executing
+ Central control – the ability to centrally control (i.e., pause, resume, stop) the operation of remotely running automations from within the Control Room

SECURE SOFTWARE DEVELOPMENT LIFECYCLE (SDLC) SUPPORT

To maximize the controls and safeguards placed on the automation environment, the basic deployment scenario described previously can be "expanded" to further deliver on Secure Software Development Lifecycle (SDLC) best practices, such as those required by FISMA, FedRamp, and PCI DSS. The resulting advanced deployment model provides three distinct RPA zones – one each for development, user acceptance testing (UAT), and production (see Figure 8). Each zone is logically separated (isolated) with different user groups given distinct roles and privileges. The dashed vertical lines represent network segmentation and firewalls.

As in the basic deployment model, the bot lifecycle starts in development. Once the BotBuilders are satisfied with the bot, UAT BotPromoters transfer the bot from the development versioning repository (SVN) to the UAT repository. The exclusive purpose of the UAT zone is to test bots for accuracy, performance, and security. Once a bot passes acceptance testing, a production BotPromoter transfers it to the production zone. At this point, it attains production status and becomes available to RPAOperators for use with production applications. At each step in the process, checks and certifications are performed by distinct administrators with different roles and privileges. Strict separation of duties and multi-layer controls are built-in by design to ensure the Digital Workforce is reliable, scalable, efficient, secure and compliant.

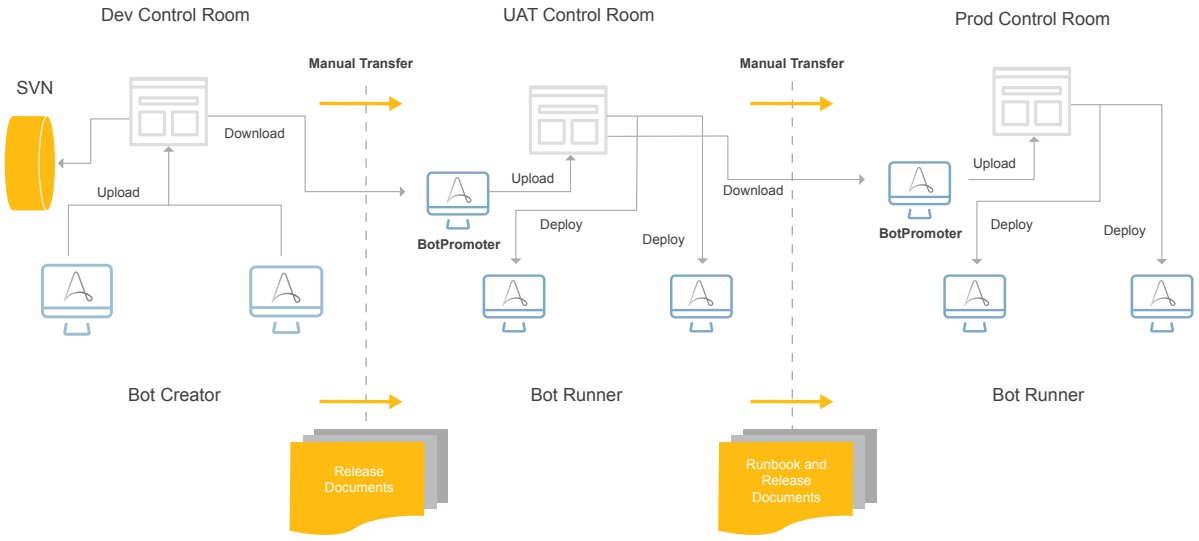

Figure 8: Advanced Deployment Model for full SDLC Support

LOGGING AND MONITORING

Comprehensive audit logging, monitoring, and reporting capabilities are essential components of the security architecture for any high-profile IT solution. Automation Anywhere Enterprise is no exception.

Across the platform, event details (who, what, when, where, and outcome) are automatically captured for 60+ types of user/entity actions – including the creation, modification, enablement, disablement, and removal of users, bots, Bot Creators, and Bot Runners. Non-repudiation is achieved via a combination of automatic capture, binding of each activity to a specific identity, and a default, read-only policy. RBAC can also be employed to tightly control which roles have visibility to audit logs in the first place.

From a monitoring perspective, automated dashboards and reports are accessible within the Control Room and can be customized to identify and alert abnormal activities (or any other detail the automation or security team decides to be of interest). In addition, the ability to export logs supports the use of other analysis, reporting, and incident investigation/response infrastructure already in use by the organization – such as SIEM, UEBA, and advanced analytics tools.

ADDITIONAL ENTERPRISE SECURITY AND RESILIENCY CAPABILITIES

Automation Anywhere Enterprise further supports enterprise security and resiliency objectives with:

+ A distributed (and flexible) component architecture that is capable of seamlessly "fitting in" to an organization's existing high availability/disaster recovery (HA/DR) infrastructure and processes
+ An integral version control system (Apache Subversion) that, in conjunction with the platform's extensive RBAC features, is capable of implementing and enforcing a highly rigorous change management policy and processes
+ Tools such as the Hibernate and ReactJS frameworks during the development of platform code to help eliminate susceptibility to common attacks (such as SQL Injection and Cross Site Scripting)
+ A security plan/protocol for code development that requires ongoing multi-tool, multi-layer scanning to detect and eliminate software vulnerabilities

More details on these and the many other controls, safeguards, and security capabilities that are part of the Automation Anywhere Enterprise can be found here: Automation Anywhere Enterprise: Security Architecture.

Robotic Process Automation holds great promise for modern enterprises looking to drive down operational costs, enhance customer satisfaction, and gain an edge on the competition. As the market's leading, Intelligent Digital Workforce platform, Automation Anywhere Enterprise helps ensure maximum achievement of these and other benefits by delivering not only the reliability, scalability, and usability features needed for success, but also the enterprise-grade security required to preserve the confidentiality, integrity, and availability of the entire automation environment.

For more information about Automation Anywhere Enterprise, visit: https://www.automationanywhere.com/products/enterprise.