How Blue Prism Sets the Standard for Secure Robotic Process Automation

blueprism.com

Introduction

Striking the right balance between business agility and security management is critical for every organization. Every time you introduce a new technology touchpoint to your company — whether it is Cloud-based or internet-enabled — you must address a new security risk. At the same time, for innovation and competitiveness to prosper, control of Robotic Process Automation (RPA) technology must be placed with business leaders throughout the enterprise.

Achieving this with total confidence requires an automation platform that is easy to use, yet still strictly adheres to the high compliance and security standards that each industry demands. The cost of failure in some sectors can result in the incurrence of huge fines and even lead to imprisonment.

> **The built-in security credentials of Digital Workers, mean that they're trusted to operate within the most demanding enterprise environments.**

Blue Prism's connected-RPA technology is unique because it was designed to perform process automations in the same way humans do — only more secure — by deploying Digital Workers. The built-in, security credentials of Digital Workers, mean that they're trusted to operate within the most demanding enterprise environments. Although Digital Workers are run by business users through a collaborative platform, they still operate within the full governance and security of the IT department, including the most regulated business sectors.

Blue Prism's connected-RPA technology solved the 30-year integration challenge of system interoperability by re-purposing the user interface as a machine interface. This innovation enables Digital Workers to use and access the same IT systems and mechanisms as humans – so they can automate processes in any past, present or future system, independently of machine APIs.

With connected-RPA, business users train and run Digital Workers without coding, so the system infrastructure remains intact, and although Web services and code stages are available, they are rarely required.

For connected-RPA to deliver security, longevity and resilience at scale, automations should be carefully planned, modeled and designed. This means that business users can create automated processes by drawing and designing process flowcharts that are intuitive and can be used by the Digital Worker to automate a task. Documentation of a task becomes the actual task; change the documentation and the task is instantly changed. The process models run by the Digital Worker are made explicit in the process flowchart for each automated process. The process flowchart is subject to audit and change control. This approach is highly secure and compliant, as all documentation is securely managed within the connected-RPA platform.

Connected-RPA also enables business users to collaborate by adding their automations into a central pool of capability that is managed and reused by the entire business. The Digital Workers' decisions and actions are centrally captured and audited too, and so is their training history conducted by humans. A crucial part of the process, this gives a comprehensive audit of all activity across the entire connected-RPA platform.

Organizations should only consider RPA vendors that can demonstrate the highest level of Veracode Verified accreditation — a third-party credential that validates a company's secure software development processes. Blue Prism was the first RPA vendor to achieve Verified Level 5. This certification not only demonstrates Blue Prism's focus on providing an authentically built, enterprise-grade, secure solution, but is also part of the company's intrinsic product development methodology.

VERACODE
VERIFIED
CONTINUOUS

Secure Software Development Lifecycle

Blue Prism's product development methodology follows a comprehensive security assurance process that informs every stage of design, and development of our software and services. This approach helps us predict, identify, and mitigate vulnerabilities and threats. We continually examine this approach, leveraging best practices to ensure that Blue Prism remains highly secure.

Certifications and Compliance

Enterprises that benefit the most from RPA include those that are the most concerned with compliance and data security procedures, for example, insurance companies, banks, financial institutions, government agencies, and healthcare providers. They expect their RPA providers to meet cybersecurity and information control standards and policies. Blue Prism supports Payment Card Industry Data Security Standards (PCI-DSS), Health Insurance Portability and Accountability Act (HIPAA) and Sarbanes-Oxley Act (SOX) compliant processes, with controls in place to provide the necessary security and governance.

Blue Prism has contracted with Veracode to undertake regular product vulnerability analysis. Veracode offers impartial, reliable and independent verification of application security and vulnerability, using industry best-practice security methodologies, such as:

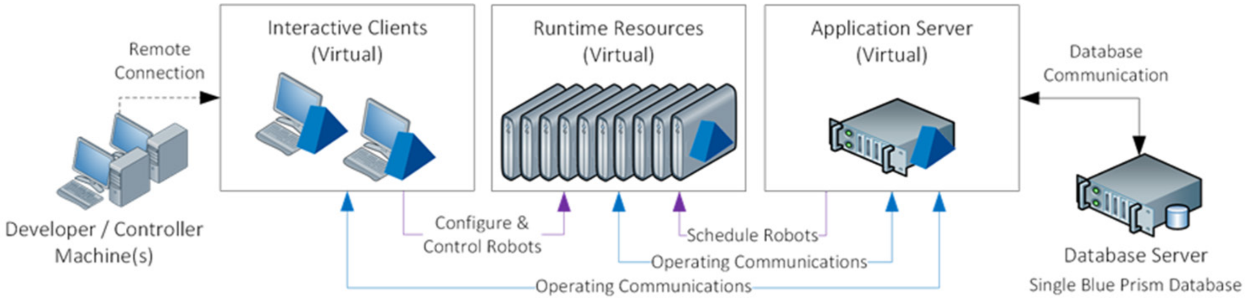
- PCI DSS: The PCI DSS are a set of technological, administrative and procedural rules that apply to the storage and processing of identifiable cardholder data, in order to ensure secure, standardized solutions are used across the industry and to minimize the likelihood of fraud. Blue Prism is optimized to enable customers to implement Robotic Process Automation as part of a PCI-compliant solution.
- PCI PA-DSS: The PCI Payment Application Data Security Standard (PA-DSS) requirements are derived from the PCI DSS requirements and Security Assessment Procedures.
- OWASP: The Open Web Application Security Project (OWASP) Top 10 is a non-profit organization dedicated to providing unbiased, practical information about application security, and represents a broad consensus on the most critical Web application security flaws.
- The 2011 CWE (Common Weakness Enumeration)/SANS Top 25 Most Dangerous Programming Errors is a list of the most significant errors that can lead to serious software vulnerabilities. The errors on this list occur frequently and are often easy to find and exploit. They are dangerous, as they allow attackers to take over software, steal data, or prevent the software from working at all. The CWE/SANS Top 25 is a list of flaws so prevalent and severe that no non-Web applications should be delivered to customers without evidence that the software doesn't contain these errors.
- CERT Secure Coding: Writing secure code helps companies avoid the software defects most likely to cause exploitable vulnerabilities. The Software Engineering Institute (SEI) CERT C Coding Standard (2016 Edition) identifies the root causes of today's most widespread software vulnerabilities, shows how they can be exploited, reviews the potential consequences, and presents secure alternatives.
- HIPAA: HIPAA is a set of US federal legislative requirements for the healthcare industry and includes, among other things, standards and requirements for the administration, management, storage, and transmission of Protected Health Information (PHI).

Industry best practice security methodologies:

- PCI DSS
- PCI PA-DSS
- OWASP
- 2011 CWE/SANS Top 25
- SEI CERT C Secure Coding Standard

Architecture

Blue Prism is most commonly hosted in a private cloud (also referred to as "on-premises") or in a public cloud. While the execution of Blue Prism is business-led, it is highly recommended that the platform is deployed, managed and governed by IT.


Remote Connection
Interactive Clients (Virtual)
Runtime Resources (Virtual)
Application Server (Virtual)
Database Communication
Developer / Controller Machine(s)
Configure & Control Robots
Schedule Robots
Operating Communications
Operating Communications
Database Server
Single Blue Prism Database

The basic components of the Blue Prism architecture

A standard Blue Prism architecture is comprised of four key components:

- Blue Prism Runtime Resource: Virtualized instances of a typically standard, end-user desktop responsible for running the automated processes, commonly referred to as 'Digital Workers.' These components also typically require enhanced physical and remote access security.
- Blue Prism Interactive Client: End-user desktop build (physical or virtual) that facilitates the setup, development, configuration, scheduling, and monitoring of Blue Prism processes across the environment. Typically virtualized in the data center alongside other Blue Prism components, this build can be deployed directly onto end users' desktops.
- Blue Prism Application Server: The Blue Prism Server service marshals all connectivity between the Blue Prism components and database. Key features enabled by this component, which is typically provisioned as a virtual Windows Server include: secure credential management, database connection marshalling, data encryption, and scheduled process execution.
- SQL Server Database: A Microsoft SQL Server database is used as a centralized repository that holds process definitions, logs, audit, and user information. Connection from the Blue Prism components exists via the Blue Prism Application Server.

Encryption

DATA AT REST

Data at rest refers to inactive data stored physically in any digital form. Blue Prism only uses recognized encryption standards and includes Federal Information Processing Standard (FIPS)-

compliant options. The end user can choose the algorithm, generate the encryption keys, and dictate where the key is stored. Tools exist within the Blue Prism product to facilitate the rotation of encryption keys.

User configurable encryption key management:

The following information explains how the encryption key used for user-configurable encryption is generated and where it will be stored:

- Blue Prism Application Server (recommended): The encryption key is stored on the Application Server, and the key must be manually deployed to each Application Server within the environment. This is the most commonly selected scenario as it ensures the key is stored separately from the encrypted data. It supports clients that connect via an Application Server.
- Database: The encryption key is stored in the Blue Prism database. This is appropriate for scenarios where there is not an Application Server deployed. It supports clients that connect directly to the database and those that connect via an Application Server.

Some information in the Blue Prism database is stored as encrypted data within the rows on the tables. This ensures that if the database was compromised, the data would still need to be decrypted to be exposed. By default, this information is encrypted symmetrically using AES Encryption. Additionally, database encryption can be provided by the default Microsoft encryption mechanism. Transparent Data Encryption - TDE but must be implemented by the end user.

DATA IN USE

Data in use refers to active data stored in a non-persistent digital state, typically in computer random access memory, CPU caches, or CPU registers.

Blue Prism uses Microsoft's Secure String functionality that is built into the .Net framework. A secure string represents text that should be kept confidential, such as by deleting it from computer memory when no longer needed. Blue Prism Safe String is a wrapper around Secure String, which is built into the .NET Framework. It ensures that when sensitive information, such as a password, is being processed in memory, it is held in a secure container that cannot be compromised — even if an attacker was able to inspect a memory snapshot of the application at that time no sensitive information would be exposed..

DATA IN MOTION

Data in motion refers to data that is traversing a network or temporarily residing in computer memory to be read or updated. Blue Prism recommends that certificate-based encryption is applied by manually deploying an appropriate certificate to each Runtime Resource and updating the device's start-up parameters.

TCP connections:

Blue Prism is built upon the .NET Framework version 4.7. The .NET Framework 4.7 and later versions default to the host operating system configuration, automatically choosing the best security protocol and version. This applies to TCP-, WCF- and HTTP-based communication. Available protocols and ciphers are managed by the end user or are automatically handled through Microsoft security updates. Blue Prism 6.1 through version 6.5 TLS1.2 were enforced for TCP and HTTP protocols; this was changed to use the above in version 6.6 and beyond.

WCF Connections:

The WCF connection used in Blue Prism has the following user selectable encryption methods:

- Message encryption and Windows authentication
- Transport encryption and Windows authentication
- Transport encryption
- None (For debug purposes only)

The WCF configuration used for message level encryption is created programmatically and uses the .NET standard encryption scheme of AES256 which cannot be altered. When the Blue Prism components are deployed within an Active Directory Network Infrastructure and configured with appropriate domain trusts, communication message security is enabled by default for inter-component communication. Further information on securing connections by enabling message security is provided within the Securing Network Connectivity Data Sheet.

Third-party Cryptographic Functionality

Cryptographic functionality used by Blue Prism is provided by the following third-party products:

- Microsoft Windows Operating System
- Microsoft .Net Framework
- Microsoft Windows Communication Foundation (WCF)
- Microsoft SQL Server

Database connections: This is the read/write connection between the Application Server and database. Certificate-based encryption is supported by leveraging SQL Server functionality which can auto-generate self-signed certificates, or leverage an existing, verifiable certificate.

OBFUSCATION

In addition to encryption, Blue Prism uses obfuscation algorithms. Obfuscation helps to reduce the risk of sensitive information disclosure by making it less clear and harder to understand and is often used to complement other existing technologies or controls.

- Cipher obfuscation: Primarily used to obfuscate Credential (Blue Prism credential manager) information
- Simple obfuscation: Primarily used for obfuscating information that is serialized/de-serialized across boundaries

- Source-code obfuscation: The Blue Prism source code is obfuscated in its majority using an industry leading obfuscation tool. Source code obfuscation dramatically reduces the risk of successful reverse engineering and malicious patching by increasing the complexity of the task and the time needed to carry it out.

FIPS 140-2 COMPLIANCE

With version 6.6, Blue Prism can be used on devices that enforce FIPS-compliant algorithms. To implement this, several changes have been made to ensure that Blue Prism adheres to FIPS. The Blue Prism application server, interactive client, and Runtime Resources now check to see if the group policy to use FIPS compliant algorithms for encryption, hashing, and signing is enabled. If it's enabled, non-FIPS compliant encryption schemes cannot be selected in the Encryption Scheme and Work Queue system settings on the interactive client. They also cannot be selected when configuring an encryption scheme for the application server and any AutomateC commands that use non-FIPS-compliant options cannot be run.

Authentication

ACTIVE DIRECTORY INTEGRATION

Using the .Net System.Security and SystemDirectoryServices namespaces, Blue Prism provides a range of enterprise-strength capabilities by leveraging Active Directory (AD) Domain Services. Active Directory is used to manage and control user access to the Blue Prism platform in-line with existing security policies, which is the recommended approach for enterprise deployments. Furthermore, Active Directory can be used to provide inter-component message security.

The Blue Prism Platform should be deployed within an Active Directory Network Infrastructure to enable enterprise-strength capabilities such as:

- Single sign-on (SSO) for the Blue Prism Platform (provided by Active Directory Domain Services).
- Integrating Blue Prism with Active Directory for SSO leverages the functionality of Active Directory to validate users' access to the platform. This approach not only simplifies the log-on process, but also aligns user access controls with existing network security policies. This requires the users' AD accounts, the Blue Prism Server(s), and all Blue Prism devices that will be accessed by users (i.e., the Interactive Clients, and possibly the Runtime Resources) to reside within a common Active Directory forest.
- Runtime Resources domain account authentication. Where the Blue Prism Runtime Resources are configured to authenticate using a domain account, they can utilize SSO methods to authenticate with the business applications and systems used as part of a process automation.

LOGIN AGENT

The login agent feature allows the remote initialization and closure of user sessions on a Runtime Resource. This ensures that a Runtime Resource can be placed in a “logged-out” state when not required, which prevents any unintended interactions. The login agent takes login credentials from the secure Credentials Manager.

MULTIFACTOR AUTHENTICATION

Multifactor Authentication (MFA) grants access after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism:

- Something only the user knows
- Something only the user has
- Something only the user is

Digital Workers:

The requirement for MFA is to avoid human vulnerabilities. However, Digital Workers are by their very nature, more secure than humans. For example, Digital Workers:

- Operate in a secure environment within the client’s own firewall
- Don’t access the systems and networks from all around the world over internet connections
- Don’t write down passwords or disclose them like humans do
- Aren’t vulnerable to phishing, shoulder surfing or violent threats
- Can be built to change their passwords frequently and easily deal with long and complex passwords

Interactive clients:

Blue Prism does not currently offer native support for MFA within the product (i.e., logging into the product using at least two forms of authentication). This can be delegated to the operating system and performed when the user logs into the software - if the SSO is configured within Blue Prism.

Third-party applications:

The requirement for MFA of target applications is entirely dictated by the capability of the target application and whether it will support it. Where it’s required, physical tokens are not appropriate but there are several alternative approaches available:

- Software tokens: Many token-based authentication schemes come with an API or “software token” option, and we can use this instead of the physical token. Some examples of soft token options include SMS via a virtual mobile, OTP, and so on. Although it is the same software and security server, the hardware token is emulated via software sitting on the virtual machine where the Digital Worker is located. There are several options for MFA available on the Blue Prism Digital Exchange (DX): https://digitalexchange.blueprism.com.

- Smart cards: Some organizations use other forms of two-factor authentication, including Smart Cards. Blue Prism has extensive experience automating the authentication process with a hardware smart card device.

However, Blue Prism recommends that any requirements for MFA in these circumstances are reviewed to consider their necessity for Digital Workers.

Authorization

There are several interactions for which user accounts are required as part of a Blue Prism implementation. Examples of these include:

- Those used by the Runtime Resources to authenticate against the network or workgroup
- The Runtime Resources used to access and automate the target applications
- Those used by Blue Prism controllers and developers to configure, develop, release, and deploy processes and the associated queues, schedules and settings

Security should also be considered for:

- Access (including remote access) to the various Blue Prism components, e.g., the Application Server or Runtime Resources
- The logical access permissions granted to each users' actions, available to them within the Blue Prism environment

USER ACCOUNTS: RUNTIME RESOURCE NETWORK AUTHENTICATION

If user accounts are used when Runtime Resources are authenticated to the domain or workgroup considerations include:

- Access (including remote access) to the various Blue Prism components, e.g., the Application Server or Runtime Resources
- The logical access permissions granted to each users' actions, available to them within the Blue Prism environment

USER ACCOUNTS: TARGET APPLICATIONS

It is necessary for Blue Prism Runtime Resources to have appropriate access to each line of business or automated third-party applications. It is recommended that a user account with appropriate permissions be made available for each of the Runtime Resources that will have a concurrent connection to a given application. Support is also provided for Blue Prism Runtime Resources to use shared credentials.

The credentials for these user accounts are securely stored, independently of the process definition, within a centralized Credential Management repository. To prevent unauthorized use within the environment, access to specific credentials is restricted to specific Runtime Resources, processes and users. Blue Prism processes can be configured to change these application password(s) periodically, which ensures the credentials aren't known by human operators.

USER ACCOUNTS: BLUE PRISM USERS (CONTROLLERS / DEVELOPERS)

By default, Blue Prism's native authentication is used to manage user access to the Blue Prism application and for assigning appropriate controls and permissions to each user. Alternatively, Blue Prism can be integrated with Active Directory Domain Services for controlling and configuring user access and control.

Irrespective of the type of authentication selected, user access is role-based and configured independently for each environment, allowing specific users to have different access dependent on the environment and restricting any single user from having total access across all environments.

The logical access permissions that need to be configured are part of the project initiation and Blue Prism supports use of a mixture of bespoke and out-of-the-box security roles to allocate each user the appropriate access in each environment.

Examples of roles that are often reviewed as part of this definition are:

- Create, read, edit, delete processes
- Create, read, edit, delete business objects
- Compare, export, import processes or business objects
- Define release package, create release
- Create, edit, delete schedules
- Full or read-only access to queues/sessions
- Access to define system settings, users, credentials, etc.

It is necessary to establish any logical access restrictions that will be implemented to provide an appropriate level of control and governance across the various environments. These may include:

- Preventing any development from taking place in the production environment
- Restricting which users can migrate processes (and associated items) between various environments
- Identifying which users will be responsible for the settings, configuration and user access
- Identifying which users will have access to the various types of audits and logs

MULTI-TEAMS

The Multi-team Environments (MTE) function enables organizations to model increasingly complex security configurations within Blue Prism by extending the existing role-based access controls to enable more granular configurations. These capabilities enable organizations to share Blue Prism assets, such as Business Objects and Runtime Resources, with multiple teams within a given Blue Prism environment. The MTE function enables permissions to be assigned by asset type and hierarchical structure of the assets. For example, users who are members of a team may have full access to some business objects but may only have the ability to view or execute others.

Credentials Management

CREDENTIAL MANAGER

The Credentials Management functionality provides a secure repository for login details required to access target applications by the Runtime Resources. Credentials are stored in the Blue Prism database and are encrypted using the encryption scheme defined by the client. The encryption key is stored separately, on the Blue Prism Application Server machine and is used to provide credentials to validated clients.

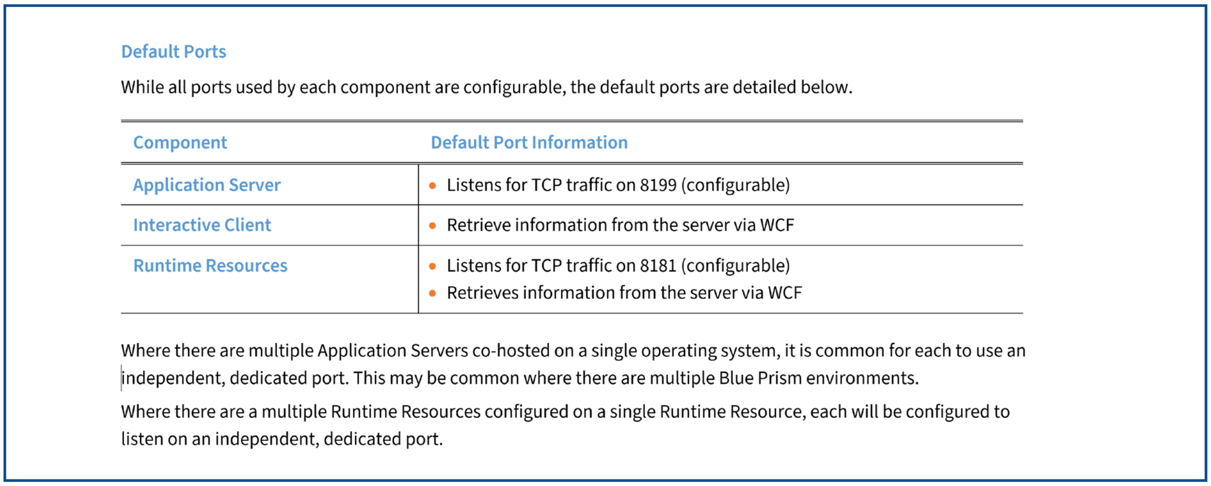
CONNECTING TO CYBERARK

The Blue Prism CyberArk Integration allows for credentials to be retrieved from the CyberArk Credential store, while retaining the controls over their context within the Blue Prism environment, using existing functionality. The integration is available on the Blue Prism Digital Exchange (DX): https://digitalexchange.blueprism.com/dx/search?keyword=cyberark. Alternative integrations are also available on the DX.

Network Connectivity

To ensure compatibility with evolving network infrastructures, Blue Prism can be deployed in environments that utilize IPv4 or IPv6 network protocols for all connections, as well as those that use a hybrid approach, utilizing a combination of both protocols. This enables all Blue Prism components — Runtimes, Clients, Application Servers — to connect using the preferred or most suitable method.

There are several communication channels within the Blue Prism platform, such as the connections to the database and the Runtime Resources. All are natively encrypted or may have encryption applied through certificates. For more information on communication between components, contact Blue Prism for our reference architecture guide.



Default Ports

While all ports used by each component are configurable, the default ports are detailed below.

Component	Default Port Information
Application Server	• Listens for TCP traffic on 8199 (configurable)
Interactive Client	• Retrieve information from the server via WCF
Runtime Resources	• Listens for TCP traffic on 8181 (configurable) • Retrieves information from the server via WCF

Where there are multiple Application Servers co-hosted on a single operating system, it is common for each to use an independent, dedicated port. This may be common where there are multiple Blue Prism environments.

Where there are a multiple Runtime Resources configured on a single Runtime Resource, each will be configured to listen on an independent, dedicated port.

Logging and Monitoring

LOGGING AND AUDIT

Session logging

Blue Prism processes contain several steps that the Runtime Resources follow as part of executing the process. These stages can represent a variety of actions, including: calculations, decisions, reading data from a user interface element, and executing a sub-process or action. Sessions are used by Blue Prism to record all the appropriate stages, followed by a Runtime Resource, as part of executing a business process. The amount of logging for each stage is configured as part of the process design.

Work queues

Work queues provide the storage and workflow capabilities for processes. Each work item represents an individual record — its data, status and history. A work item has several statuses, including: pending, deferred, locked, completed, and terminated. If a work item is terminated by the process, it may be retried automatically; each queue can be configured with a set number of automatic retries.

Audit logs

Blue Prism's audit trail is centrally stored and tamper-resistant, so no one can alter or falsify it. In the event of non-compliance or audits, this function delivers irrefutable non-repudiation.

Audit Logs are used to record the following actions:

- Login/Logout
- Changes to environment-wide settings
- Create/update/delete of business objects, processes and queues

When recording changes to processes and objects, all change details are captured to allow for comparison or rollback.

Schedule logs

Logs are created for each schedule and record the time and outcome for all tasks and sessions within that schedule.

MONITORING AND ALERTING

Platform monitoring

The Blue Prism infrastructure is comprised of several different components, each of which can be monitored and polled to verify availability and responsiveness. When monitoring the Blue Prism components, standard third-party tools and techniques can be used to evaluate the following:

- Health of allocated hardware (e.g., disk space, CPU utilization, network connectivity)
- Availability of specific windows services (e.g., service started, responding on the appropriate port)
- Windows Event Viewer entries

Alerting

There are several alert types that can be configured to notify relevant parties of anything, from exceptions to process completion. Alert types include:

- Process Alerts: These notify specified users when certain actions occur for selected processes within the Blue Prism environment and are configured on a per-user basis. Users can select which processes they want to monitor, actions they want to be told about, and how they want to be notified.
- Schedule Alerts: These notify specified users when certain actions occur for selected schedules within the Blue Prism environment and are configured on a per user basis. Users can select which schedules they want to monitor, and how they want to be notified. Also, they can choose whether notifications are required at the schedule, or more detailed schedule-task level.
- Custom Alerts: Where additional or specific alerts are required, it is possible to design custom alert notifications into any process.

APIs

The Web API functionality provides an interface for configuring native interactions with systems and services that provide published HTTP APIs. The most common of these is RESTful Web Services. The Web API Services feature allows Blue Prism processes to interact with these services and either provide data or consume the data or services provided by these external systems within an automated business process. The features provided natively by the Web API functionality allow the most common services to be automated by Blue Prism, and these capabilities can be extended using code stages to cater for bespoke, or complex data structures and authentication mechanisms.

Controls

THE ROBOTIC OPERATING MODEL

The Blue Prism Robotic Operating Model (ROM) is a framework designed to help users effectively manage their RPA deployments and then successfully scale. The ROM includes advice and guidance on controls, including Logical Access Models and process governance. Find out more at https://blueprism.com/rom/

LOGICAL ACCESS MODELS

Blue Prism recommends that, from the beginning, each organization create and implement its own Logical Access Model (LAM). This should be included as part of any Blue Prism deployment. The default user roles defined within the product should be replaced with user roles defined by the organization's own LAM. This action should be carried out for each Blue Prism environment, i.e., Development, UAT and Production.

Please note that the Runtime Resource and System Administrator user roles cannot be changed. The process of creating or updating the LAM should involve all stakeholders, including the Head of RPA, the RPA Governance Board and IT team. The segregation of duties must be considered within the organization, too. A LAM template and guide is provided as part of the ROM.

CHANGE MANAGEMENT

When deploying and maintaining a Digital Workforce, it's recommended that organizations follow their existing change control processes. The ROM provides guidance on delivery best practices, outlining how processes are defined, designed, built, reviewed, tested and released.

Additional Considerations

PENETRATION TESTING

Blue prism is subjected to 3rd party penetration tests performed within a "best practice" environment. Due to the subjective nature of these tests, and the unique variables in each client environment, the reported results should only be used as a guideline. More information around the testing methodology and results can be found in the latest Blue Prim Veracode application security report.

Conclusion

Blue Prism has always made security a key component of its connected-RPA technology, which is evidenced by being the first Veracode Verified Level 5 RPA vendor. Offering the most complete, enterprise-level security, Blue Prism's centralized, data-center-hosted approach ensures that its IT-governed, business-run platform is the most reliable and secure. Encryption ensures data is protected, with additional encryption options easily deployable. Flexible and robust authentication and authorization capabilities ensure that organizations can deploy a digital workforce that's aligned with their standard operating procedures. Extensive logging and alerting options ensure complete visibility and audit trails for both Digital Workers and Blue Prism users.

All these compelling features are underpinned by our industry-leading ROM's strong governance and controls that include access models and delivery methodologies. Ultimately, connected-RPA provides the most secure collaboration platform for human and Digital Workers to safely deliver real digital transformation.

blueprism®

About Blue Prism

As the Robotic Process Automation (RPA) pioneer, Blue Prism is the trusted, secure Intelligent Automation choice for the Fortune 500 and public sector. Today, Blue Prism's connected-RPA joins operational leaders with accessible, advanced cognitive technologies and a community of experts to bridge the gap between human and digital workers, while strengthening the capabilities of the 21st century workforce.

More than 1,000 major enterprises leverage connected-RPA on-premises, in the cloud, or as an integrated solution in a hybrid cloud environment, empowering their people to automate billions of transactions while returning millions of hours of work back to the business.

Visit **www.blueprism.com**.