One Identity Safeguard secures and automates access to privileged credentials for Blue Prism RPA

Blue Prism's Technology Alliance Program (TAP) partnership with One Identity adds secure privileged access to Blue Prism Robotic Process Automation (RPA) to enhance security, mitigate the risk of a security breach and make it easier to achieve compliance. This integration with One Identity Safeguard adds the critical skill of automating, controlling, and securing digital workers and Blue Prism developers' access to privileged credentials when using Blue Prism Intelligent Automation, giving enterprises enhanced security within a Blue Prism Digital Worker's defined workflow.

Increase Blue Prism RPA security with Privileged Access Management

RPA software interacts directly with business applications and mimics the way applications and humans use credentials and entitlements. This can introduce significant risks when the software robots automate and perform routine business processes that need access to privileged credentials. Ensuring that those privileged credentials are provided and managed in a secure manner reducing the risk of breach through compromised access to confidential customer and business data is a top-priority for the development and adoption of RPA.

Traditionally privileged credentials are stored directly in the credential manager of the RPA tooling, allowing digital workers to perform business activities across multiple systems. The Blue Prism credential manager is encrypted, however there is no way to automate password rotation or track when and where credentials were used.

In order to enhance security and achieve compliance, you need the privileged accounts used by RPA to be securely managed according to published best practice guidelines for Privileged Access Management (PAM), which include;

- **Individual Accountability** - Each Digital Worker/Robot should be using a different service account at any given time, to prevent the compromise of all digital worker services using the same service account if one service account is compromised.
- **Password Rotation** - Each service account should have its passwords managed in accordance with domain account policies (changing every 90 days for example).
- **Audit Trails** – All privileged activity performed by RPA should be tracked and securely stored to ensure compliance.

The administrative overhead of manually managing large numbers of separate privileged domain accounts, and the passwords that Digital Workers/Robot use for process execution, can be a nightmare. With One Identity Safeguard, it doesn't have to be.

How it works

With One Identity Safeguard you can automate, control and secure the process of granting privileged access to Robots. Passwords can be automatically rotated according to your compliance requirements.

All activity is tracked and can easily be reviewed to see which individual or robot has had access to a system and when they had it.

In addition, Blue Prism RPA developers need to gain access to the Digital Worker credentials, in order test Blue Prism workflows along with any other privileged accounts that are used during those workflows. Using Safeguard's session management solution, you can record and monitor all actions that the developer has done, to ensure the credentials are being used properly. You can automatically log the developer in so that they never gain access to the passwords. These recorded sessions are indexed, making it easy to search for specific events or commands and simplifying audit reporting for compliance requirements.

Summary

The One Identify Safeguard Blue Prism integration enables you to implement secure best practices within your RPA environment. You can be confident that each digital worker is using the right credential for the right process, that credentials are not being shared between robots, or between developers. This brings a new level of security best practice and reduced risk to your business.

About Blue Prism

As the pioneer, innovator and market leader in Robotic Process Automation, Blue Prism (AIM: PRSM) delivers the world's most successful Digital Workforce. Blue Prism provides a scalable and robust execution platform for best-of-breed AI and cognitive technologies and has emerged as the trusted and secure RPA platform of choice for the *Fortune 500*. For more information, visit www.blueprism.com.

About One Identity

One Identity helps organizations get identity and access management (IAM) right. With our unique combination of offerings, including a portfolio of identity governance, access management, privileged management and identity as a service solutions, organizations can achieve their full potential – unimpeded by security, yet safeguarded against threats. Learn more at OneIdentity.com