cedrus
digital transformation solutions

ROBOTIC PROCESS AUTOMATION (RPA) SECURITY OFFERING

IDENTITY AND ACCESS MANAGEMENT (IAM) FOR BOTS

THE CHALLENGE

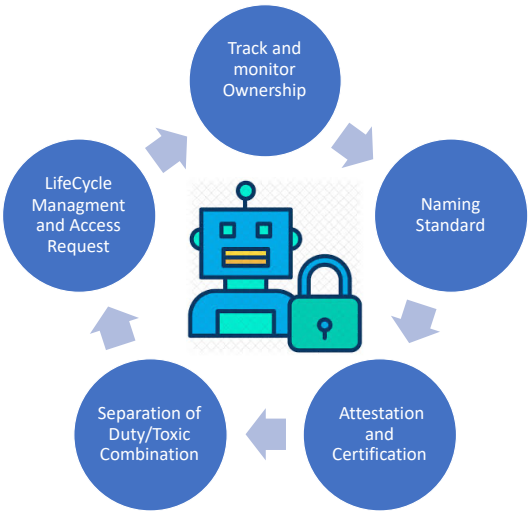
Organizations are turning to Ro(BOT)tic Process Automation (RPA) technology in order to enable efficient and error free processing of standardized tasks and accelerate scalability. While these BOTS improve performance, they have largely been left untouched by enterprise IAM programs. This causes manual account creation, tracking, and removal of system and application access for BOTs and leaves organizations exposed to security and compliance risks. In addition, BOTs need user credentials to perform tasks interactively or access data and services. These BOT credentials are often hard-coded, shared, unmonitored, and re-used. Topics that need to be understood:

- Access credential provisioning and management required for BOTs
- Identification of the responsible party for individual BOT management and access certification
- Storage and usage of credentials in BOT workflows
- Management, rotation, and expiration of BOT passwords
- BOT activity monitoring and auditing, especially if interacting with confidential or restricted data

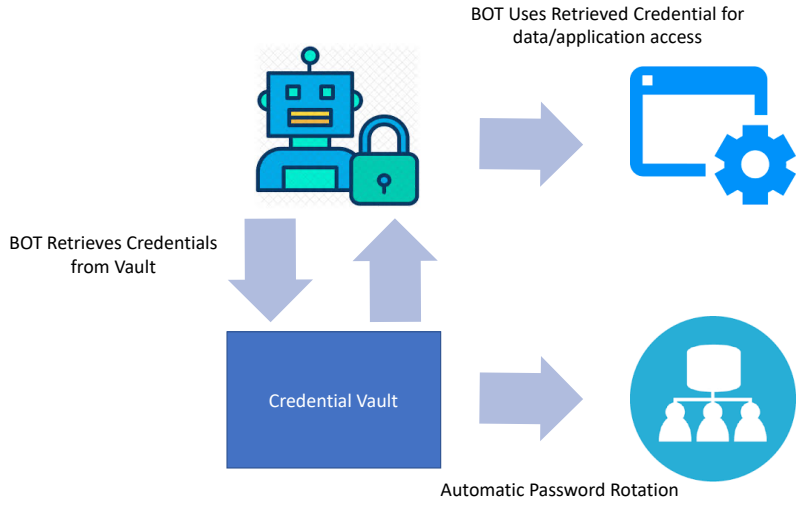
BOT credential management is essential to streamline creation / removal of BOT access, reduce audit time, and protect infrastructure from bad actors. Exploitation of BOT credentials is often difficult to detect and can be costly and potentially catastrophic.

OUR EXPERTS AT CEDRUS CAN HELP

Our systematic approach to BOT access credential lifecycle management is an integral part to our overall Business Automation practice.



BOT Identity Management and Governance



BOT Privileged Access Management

cedrus
digital transformation solutions

ROBOTIC PROCESS AUTOMATION (RPA) SECURITY OFFERING

IDENTITY AND ACCESS MANAGEMENT (IAM) FOR BOTS

THE SOLUTION

Our consultants can provide the necessary advisory skills to plan, design, and implement the appropriate RPA and BOT security approach for your organization. We will work with you to gain visibility into your BOTs and ensure that the appropriate governance policies are in place to ease operational burden as well as enforce the necessary access and monitoring controls. This will allow your organization to govern BOTs and their access to enterprise applications and data by enforcing processes like requesting, approving, and certifying access and by extending access-based policy definitions to these non-human entities.

Incorporate BOTs into your Identity and Access Management (IAM) Program
Establish a BOT Identity and Access Lifecycle Management Program
Generate a BOT entity within your Identity Governance Platform
Enforce least privilege for BOT entitlements though Role Based Access Control (RBAC)
Define and adhere to a BOT naming standard to allow of quick identification of BOTs and their functions
Implement a process identify and track BOT Identity and Access ownership, ensuring that there is a human entity responsible for the BOT and its interactions within your system and application services
Create and track Separation of Duty(SOD) / Toxic Combination Policies to ensure that your ensure your BOTs do not generate audit issues or create undue risk
Create a certification process for BOTs and ensure that the BOTs that exist in your organization are still required and that they have the appropriate level of access
Establish a vault for storage of BOT access credentials in a centralized secure repository
Setup automatic rotation of passwords for the access credentials used by BOTs
Update RPA workflows to securely retrieve credentials on demand and remove them from any code
Monitor and track any BOT sessions that have privileged levels of access to critical data or infrastructure
Record selective administrative use cases where BOT credentials are used for accountability and audit

NEXT STEPS

Cedrus experts can review your current state in an initial one hour call. We can discuss leveraging your existing IAM investments as well as establishing a baseline for BOT IAM.