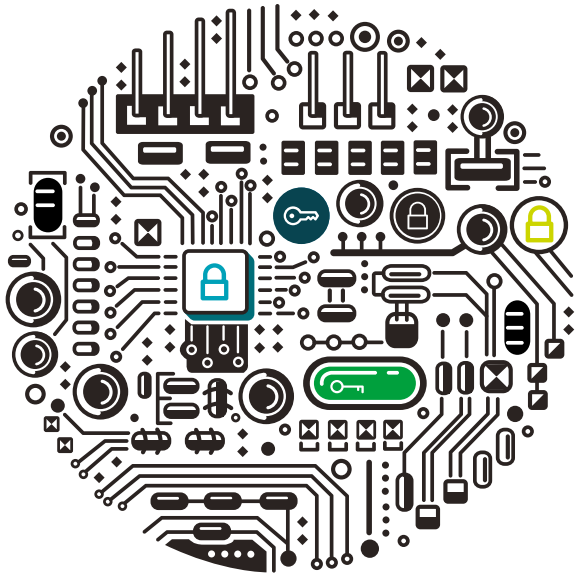
Deloitte.



IT Security for the Digital Laborer

"How do we manage the Bot and maintain IT security?"

National Security and the management of the classified data is a pressing concern for many leaders within the Defense and Intelligence agencies; with that said, technology continues to drive the way business is done not only in the average citizen's life but in the agencies that protect us. Unfortunately, there are ongoing challenges with the rapid change of technology and the outdated policies that provision newly defined technology capabilities.

Thought leading agencies, such as NASA, have allowed for opportunities to understand security limitations for Bots and establish provisions to support and maintain security of Classified and Un-Classified data.

What is digital labor?

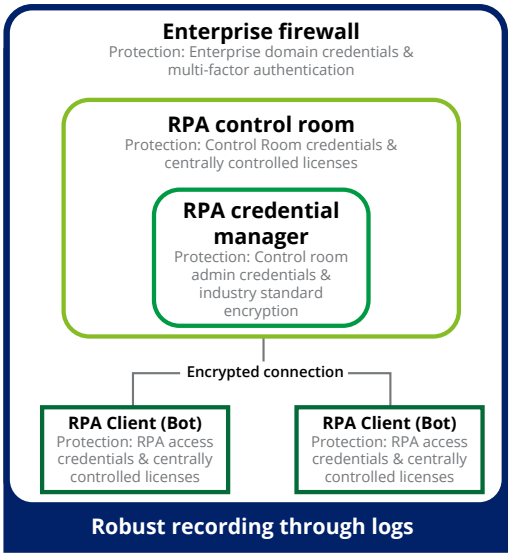
Digital labor couples today's capabilities of Automation and Data Analytics to empower the workforce as 'data users' instead of 'data gatherers'

Digital labor is an innovative solution that is driving improved efficiency and service delivery to the nation and its citizens. Digital labor should be thought of as a new category of resources that leaders can tap into a pool of digital labor that provides leaders with access to new capabilities and options to achieve mission goals. No longer are federal executives limited to the option of simply hiring new federal employees, procuring new contractors, or implementing a new infrastructure changing technology. Instead, federal executives have a new lever to pull that can combine the benefits of scalability, shorter stand-up times, and rapid ROI. [1]

What are the architectural components for Process Robotics?

The Architectural Components for Process Robotics enables an interactive yet controlled environment for the bot. These components operate as gate keepers support the security of business applications and transactional data. The Control Room operates as a centralized point between the operations/managed service (desktop/laptop) and the automation (Bot).

Robotics Process Automation (RPA) integrates into a network's security architecture with layers of protection



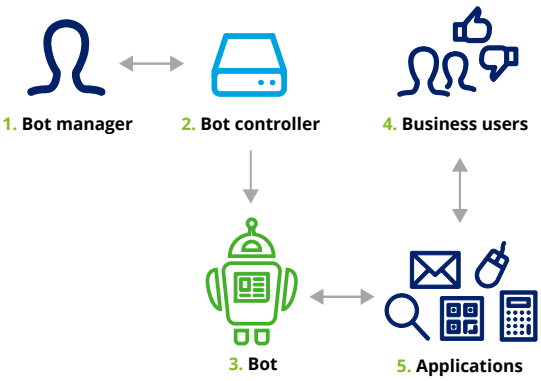
Credentials are a user-name and password for a given system

[1] Deloitte Digital Labor Whitepaper https://www2.deloitte.com/us/en/pages/public-sector/articles/process-robotics.html

What are the security requirements for a Bot?

When it comes to security, the question becomes, "How can I manage and track what resources are access what data and when?" The federal government uses PIV/CACs to provide secured access for entry into data repositories in order to perform tasks or access PII, Unclassified, or Classified data. "How can this be done for a Bot?" Leading practice is to align the Bot to a "Bot Manager"/ human entity who would assume responsibility for managing Bot access to secure data. The Bot can be provided credentials to any system via a user-name and password assignment, however; formal entry points should be consider when accessing the network servers of an agency.

1. **"Bot managers"** orchestrate robotics to ensure proper execution and help facilitate resource utilization across virtual machines
2. The **Bot controller** is used to assess jobs to ATP and to monitor their activities
3. Each **Bot** is located on an organization environment which may be virtualized or physical (i.e., desktop computer) where it interacts directly with business applications
4. **Business users** review and resolved any exceptions or escalations
5. Bots are capable of interacting with a wide range of **applications**



Process Robotics is deployed and managed from central controller to interact with a wide range of business applications. Controller can reside on a physical or virtual machine.

Security risks of data transverse via the network

Proper security controls protect against the compromising of data. Bots will have permissions to transverse the network and access certain points based on provisioning management via the Bot Manager(s) depending on access points required to complete work instructions. To minimize risks, Bot Managers should be assigned to ensure access points across multiple networks are managed and no opportunity for compromise exists. It is important to think through "what could go wrong" in the process, identify indicators of risks for when that activity may occur, and monitor for those indicators.

Prevention of a security breach

roper security controls can be set and monitored by the Bot Manager. The Bot can be designed to recognize an improper transaction or function that is outside of the work instructions. When the Bot attempts to perform a function that has not been coded for the Bot to perform, the Bot will immediately stop, produce an error, and generate the error in a log. The error log creates an audit trail of the Bot's performance and the Bot Manager is able to track and monitor the bot performance errors and analyze what caused the error. RPA incorporates an enables industry stand security through the following elements:

User roles and system access controls

Yes, it is common to remove access credentials for a Bot as you would with a human when a job has been completed. If credentials need to be reassigned or user roles to systems need to be changed in order for the Bot to perform another task, this can be done.

It is common for Bots to have multiple user roles as it performs multiple work instructions. The system administrator will control access to various systems for the Bot to perform the coded work instructions. System administrators should keep in mind that the Bot is unable to complete in-person trainings and online trainings and will require an approval authority to bypass these requirements.

Does the bot need an Authority to Operate (ATO)?

This depends on what functionality or transactions the bots can perform or execute. If a bot is programmed to mimic functionality performed or processed by an accredited system, the organization will want to consider an ATO. The data or business process affected by the Bot may also influence whether an ATO decision is required. There is no right or wrong answer but every organization should consider the extent of the analysis to which the bot introduces risk into its environment, the risk assessment level, and monitoring that is required to manage the identified risk.

Bot security key considerations

- Define process interactions and potential impacts to the organization and existing processes.
- Identify a deployment model with varying security requirements.
- Assign a custodian or Bot manager to enhance the security of the Bot.
- Understand data points for automation and security requirements.
- Baseline actual process vs. automated process and determine potential risks associated.
- Monitor and correlate anomalies with other events on the network.
- Archive or remove access privileges from Bots not in use.

Contact us:

Marc Mancher
Principal
Deloitte & Touche LLP
Tel: +1 860 488 5071
Email: jmancher@deloitte.com

Tim Li
Managing Director
Deloitte & Touche LLP
Tel: +1 240 205 2474
Email: timli@deloitte.com; com

Chris Rose
Principal
Deloitte & Touche LLP
Tel: +1 904 665 3843
Email:
christopherrose@deloitte.com

Joris Vega
Technology, Strategy, and Architecture Principal
Deloitte & Touche LLP
Tel: +1 443 939 0357
Email: jorisvega@deloitte.com

Aleshia Davis
Manager
Deloitte & Touche LLP
Tel: +1 703 568 4821
Email: aledavis@deloitte.com

Deloitte.