Data Sheet

DTS SOLUTION
CYBER SECURITY REDEFINED

Robotic Process Automation(RPA)
Cyber Security Assessment

What is RPA?

RPA is the use of a software "robot" (a program) that replicates the actions of a human being interacting with the user interface of a computer system.

Robotic Process Automation (RPA) offers immense time and cost savings, productivity and quality improvements, high customer and employee satisfaction, and drives digital transformation.

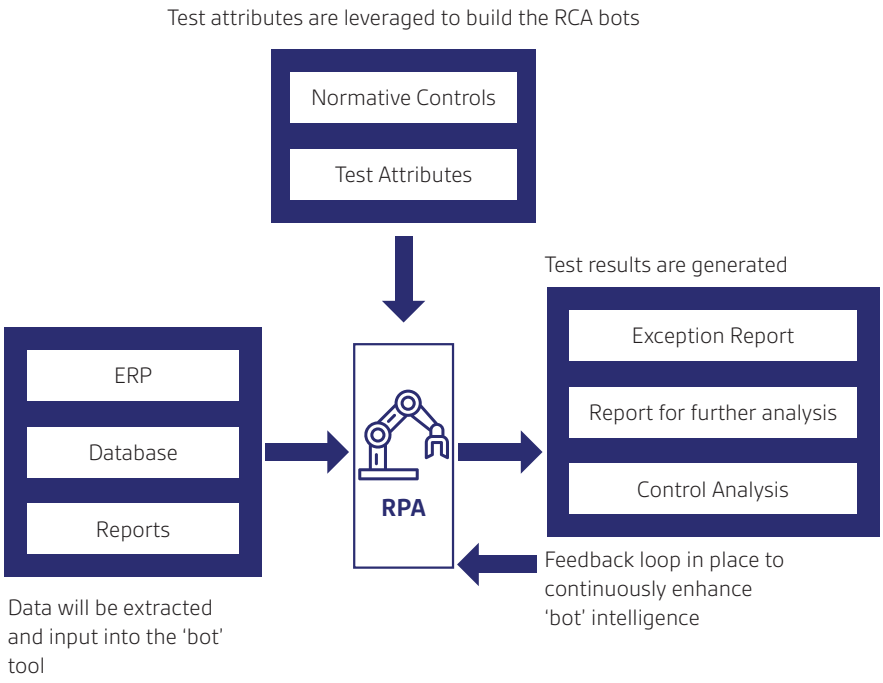
With RPA, business users are enabled to automate repetitive, monotonous and error-prone processes by themselves.

RPA Key Benefits

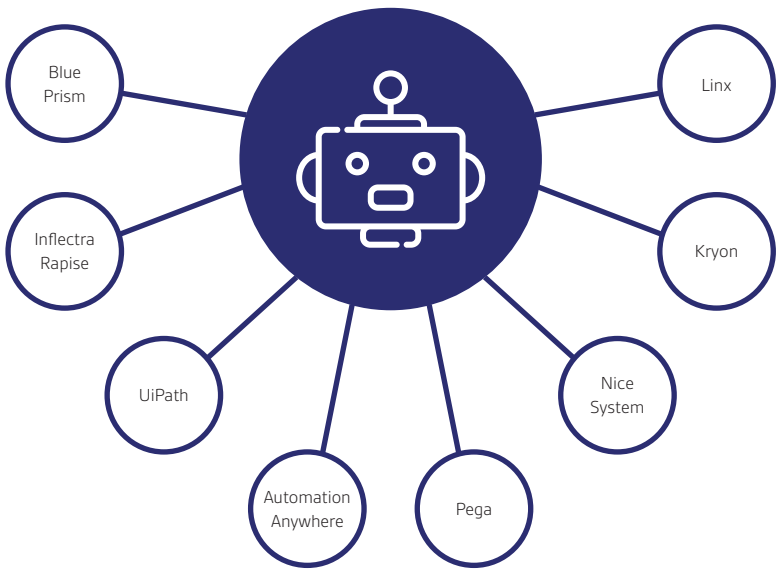
- Emulates human execution of repetitive processes via existing user interfaces
- Robots are a virtual workforce controlled by the business operations teams
- Sits alongside existing infrastructure, governed and controlled by IT

High-Level View - RPA

A high-level view of how a "bot" typically operates



RPA Tools



Robotic Process Automation (RPA) Cyber Security Assessment

RPA Security Assessment Consideration

Software & Product Security

- Security Architecture Risk Analysis of product selected
  - Analysis should include bot creation, control & running. Identify security architecture flaws in underlying product for connections across various environments, usage of virtualization methodologies, and authorization flaws
- Secure design for handling of sensitive information, including access credentials:
  - Review secure design, including data flow analysis, to confirm that controls around security are integrated in to the bot authentication, authorization, and input validation
- Implement security scanning and vulnerability testing on the robot:
  - Integrate security scanning tools as part of the bot creation process to scan code created in the backend for security vulnerabilities
  - Scan bot created for security vulnerabilities using dynamic testing or security fuzzing technology to determine security flaws
  - Verify schema for bot deployment has security considerations in place

Digital Identity & Access

- Manage user access privileges/segregation of duties risk:
  - Utilize RBAC/ABAC for robot access provisioning and access monitoring
  - Design and segregate robotic tasks/instructions to minimize overlap of SOD rulesets, allowing clean RBAC/ABAC provisioning. Enforce strict SOD rules to each robot and task/instruction
  - Implement security controls to protect sensitive data during robotic session run-time. For example, use of SSO with LDAP supports secured logon to RPA interface
- Securely manage passwords:
  - Enforce passwords consistently across robotic sessions and centralize robotic identity and access management process
  - Leverage encrypted credential manager to prevent leakage of credential

Data Identification & Protection

- Establish and monitor for sensitive data handling (including robot logging process):
  - Conduct compliance assessment to data regulations for use of robotics and automation
  - Monitoring of sensitive data processed by robotics / automation to verify compliance with usage policies
- Integrity checking of robotics and automation code:
  - Implement (likely within the COE) a process to handle system integration changes that may affect robotic operations
  - Perform robust regression testing across systems
- Improve auditability (every step could be logged) and control over error-prone manual activities that elevate risk and non-compliance

Security Operations

- Monitor for inappropriate actions/access or potential bypass of SOD rules:
  - Gather log data from controller and bot runners to provide an audit trail of activities monitoring for abnormal spikes in activity, access of systems and use of privileged accounts. For example, use of insider threat monitoring program rulesets configured for robot activities
- Establish security across the infrastructure stack for the given platform:
  - Conduct vulnerability scanning of your robotics platform and execute threat modeling exercises of robotics sessions to determine technical weaknesses process gaps

Securing the RPA Technology and Consideration

RPA Admin Credentials

- Password vaulting
- Audit logging of account activities
- Strong password policies

Server Infrastructure

- Regular patching of hardware
- Role-based access control
- Malware and data protection measures

Virtual Machines

- Regular patching of Virtual Machines (VMs)
- Change freezes while bots in operation

Bot Credentials

- Unique, strong passwords for each bot credentials exceeding standard company policy
- Limited access to only business applications needed to support bot
- Audit logging of account activities

Business Applications

- Server hardening
- Role-based access control

Monitoring and Issue Management

- Activity of robot user accounts is monitored to identify any unauthorized access
- Privileged access, including administrator accounts and super user accounts, are appropriately restricted from accessing the robot software
- Ability to make workflow changes without detection
- Inappropriate access to modify RPA logs
- Insufficient trend analysis around data volumes and run times to avoid capacity and performance issues

Securing the RPA Operating Environment

- Firewall
- Encryption of Data
- Hashing
- Data Masking
- Active Directory Integration
- Credential Management

DTS SOLUTION
CYBER SECURITY REDEFINED

DUBAI: Office 4, Oasis Center, Sheikh Zayed Road, Dubai, United Arab Emirates
T: +971 4 338 3365 | **E:** info@dts-solution.com

800 HACKED

ABU DHABI: Office 253, Al Bateen C6 Tower - Bainunah, King Abdullah Bin Abdulaziz Al Saud Street | **T:** 971 2 2076777
LONDON: 160 Kemp House, City Road, London, EC1V 2NX, United Kingdom | **T:** +44 2081230 387 (DTS)
www.dts-solution.com