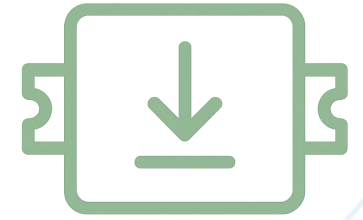ROBOTIC PROCESS
AUTOMATION

RPA - Key Technical Areas

SCALABILITY

SECURITY

EXTENDIBILITY

RESILIENCE

COMPLIANCE

Scalability

Fully centralized command & control, centrally updated re-usable objects, drag & drop design, expression builder with built-in debug, automatic process design error check, dynamic queue management, and many-to-many robot / process assignment

Control Room

Fully centralized command & control of the Digital Workforce

Digital Workers & Connectivity

Schedules & Active Queues

Filtered Work View

Work Queues

Objects : Building Blocks for Scale

By modelling the parts of the application that you are going to use first, then creating re-usable objects that interface with the system like a user, processes can be layered on top that chain together this library of objects with business rules to create flexible, maintainable processes.
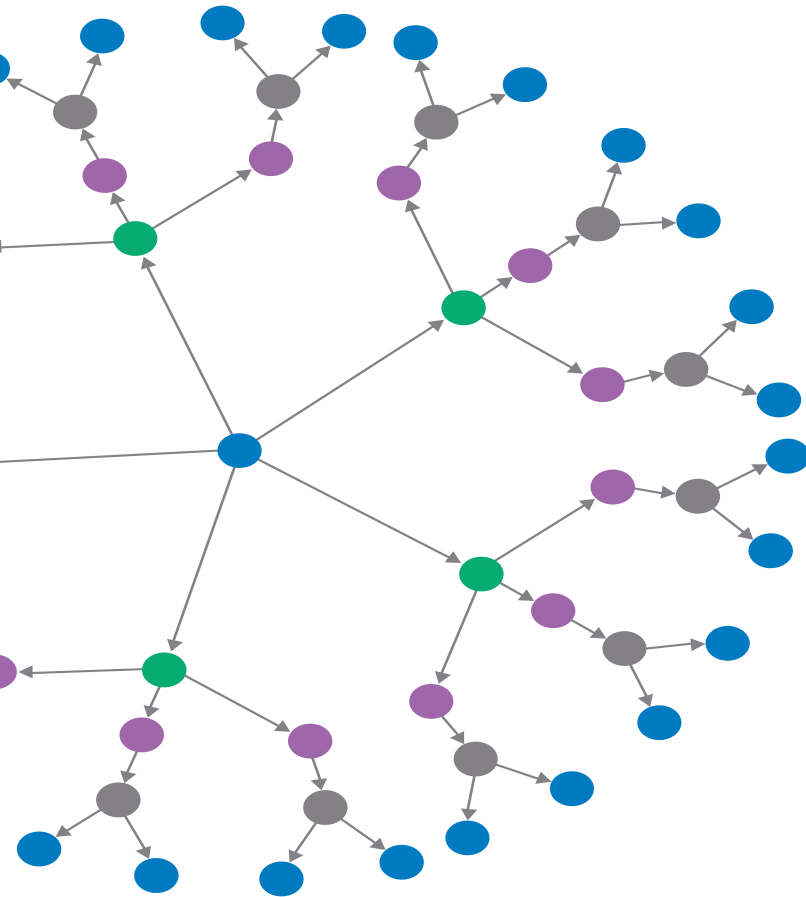
If a system changes, change the model. Once.

If an application interaction needs to change, update the object. Once.

All of the processes that use this information inherit these changes, without re-recording or rebuilding them. And processes can be written more quickly as the building blocks that already exist can be re-used in different business scenarios.

With **Synaptein**, the Total Cost of Ownership exponentially reduces over time.

Resilence

Intelligent tracking of underlying application logic, real-time logging to a central database for rollback or hot-failover, no license fee for DR, support for hybrid-cloud infrastructure, no-code exception handling, and build & debug in one studio

Object Studio

Enables the creation of re-useable RPA Objects (Application Actions) as the building blocks for the business process (Lego Pieces).

Automated Debug

Visual Element Identification

Intelligent Wait

Attribute Tracking (not screen scraping)

Process Studio : Action Stage Properties

Action Properties

Name: Save File

Description:

Business Object: Notepad

PDF
Adobe - Basic Actions
SalesOps Objects
Utility
Blue Prism MAPIEx
SOPS_Clear_Work_Queues
SOPS_iStream_Object
SOPS_SBC_Attach_And_Close
SOPS_WordInterop
SAP
SAP - Basic Actions
SAP Transactions - NGSC
Technology Specific
Mainframe
NBS Credit Search System
Utility
Utility - File Management
Utility - General
Utility Objects
Utility - HTTP - Extended

Action

Inputs Outputs

Name
FileName
Overwrite?

Group: ☐ Page ☑ Data Type
☐ View All Items

Binaries
Collections
Dates
DateTimes
Flags
Images
Numbers
Passwords

Centrally Re-Usable Objects

Stage logging: Enabled
Warning threshold: System Default Number of minutes 5 (0 to disable)
☐ Don't log parameters on this stage

Logging Options for Every Object

Action Properties

Name: Export to PDF

Description:

Business Object: MS Word VBO

Action: Add Table Row

Action to take within Object

Inputs Outputs

Name
handle
documentname
Table Number

Add Table Row
Attach Instance
Clear Clipboard
Close
Copy to Clipboard
Create Document
Create Instance
Detach Instance
Exit
ExportPDF
Find Text
Get Body
Get Footer Text
Get Highlighted Text
Get Table Cell Value
Hide
Open

Group: ☐ Page ☑ Data Type
☐ View All Items

Binaries
Collections
Dates
DateTimes
Flags
Images
Numbers
Passwords
Text
Times
TimeSpans

Process Studio

Enables SME to design, build, edit and test processes, constructed from RPA Objects.

Connected-RPA Dependency Tracking

Sub-Page Organization

Management Information Analysis

IA Skills Toolbar
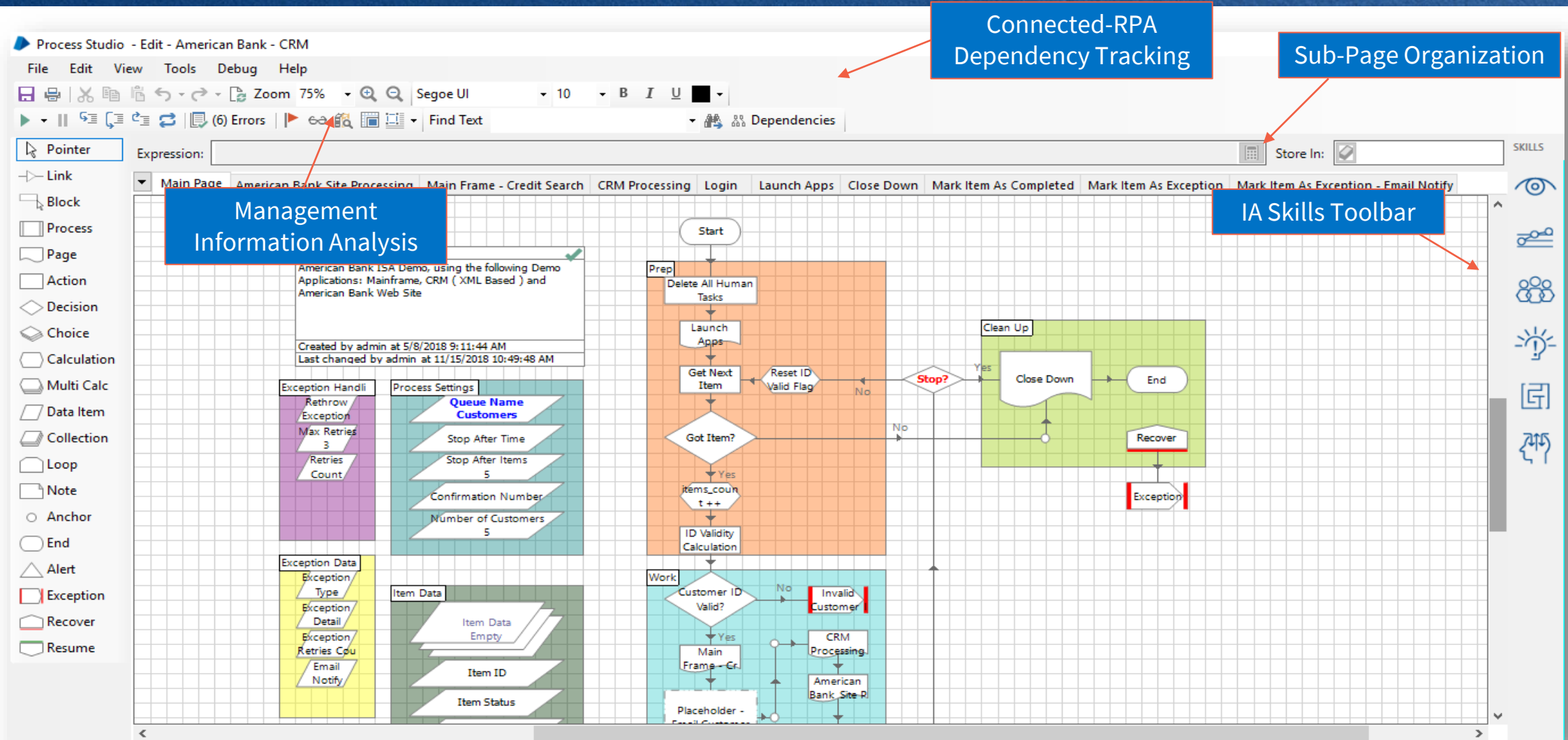
Decision Property Wizard

Continuous Improvement : Management Information

Synaptein Proprietary

Security

Military-grade credential management, integration with AD/LDAP/CyberArk, encryption of data in transit/at rest, business-level segregation of object and process permissions, decoupled build & run via granular roles-based access control, integrated password vault, disk level encryption, data masking, and integrated release management

Security & Compliance Imperatives

With the widespread adoption of Robotic Process Automation (RPA), organizations have come to understand that a digital workforce requires oversight, security, and governance safeguards similar to their human counterparts.

There are four high-level considerations business leaders must address to ensure the security and compliance of their digital workforce.

1 Infrastructural Security

What You Need to Know: At a minimum, organizations that plan to implement RPA should create an environment where their robots can operate—as well as be configured and assigned—that is free from interference, informal or casual inspection, and especially, tampering.

Action Item: Segregate processing and management environments and impose separate governing controls for each.

2 Centrally-Managed User Access Control

What You Need to Know: Looser access controls, such as team-level access, are not sufficient for fail-safe security and compliance. Access parameters that are managed per robot, process, and even specific objects are inherently more secure.

Action Items: Enable only specific users to build specific processes using specific objects. Then enable multifactor security that mandates secondary approval for all changes.

3 Systemized Activity Logging

What You Need to Know: Organizations can only ensure accountability and responsibility when 100% of all transactions for every single process are recorded in real-time and securely stored.

Action Item: Only consider RPA operating systems that systematically record 100% of every action taken and changes made—creating an unmalleable and irrefutable audit trail.

4 Irrefutable Audit Trail

What You Need to Know: Ultimately, the quality and integrity of the audit trail will not only discourage malicious activity but will provide non-repudiation.

Action Item: Implement an RPA operating system that not only logs everything, but centrally stores the log to eliminate any and all tampering of the record.

Credential Manager Overview

Environment Security

Encryption Key Held on RPA Server

Zero Retention

- Passwords are used transiently and not retained

- Runtime environment subject to rigorous physical and logical security controls
- All access audited
- Optionally secured further using RPA Secure Windows Authentication software

- Enables separation of roles/responsibilities
- Ensures no DBA can access encrypted data in isolation
- Enables different keys to be used across DTAP configurations

Recommended

Microsoft
Active Directory

- Message content security and integrity
- Single sign-on for the RPAPlatform
- Runtime Resources authenticate using a domain account

Interactive Clients
(Virtual)

Runtime Resources
(Virtual)

Application Server
(Virtual)

Database Communication

Configure & Control Robots

Schedule Robots

Operating Communications

Operating Communications

Database Server

Single Blue Prism Database

Optional

CYBERARK®

The RPA CyberArk Integration allows for credentials to be retrieved from the CyberArk Credential store, whilst retaining the controls over their context within the RPA environment, using existing functionality

Access Control Policy

- Implemented on a per credential basis, restricted by combination of user / process / resource
- Allows strict control over how credentials are used (in addition to expiry and change frequency rest requirements)

Secure Network Communications

- Passwords transmitted securely using a trusted .NET Remoting or WCF connection
- Clients & Resources can connect to Application Servers using the host name, IPv4 or IPv6.

Encrypted repository

- Passwords securely held within SQL Server database
- Encrypted using industry recognised techniques (3DES/192 or AES/256)

Exception Handling : Password Protected Screen Capture

User Permissions & Access Control

Login Agent

RPA's Login Agent provides a mechanism to assist with automating the login process for a Windows machine so that a RPA Runtime Resource can be started. This capability allows digital workers to be fully autonomous, maintain their own passwords, report they are clocked in for work, and clean-up their workspace.

A number of example RPA processes are provided within the release package:

Change Password - Resets the password for the currently logged on user and overwrites the password associated with the credential record. Provides support for configuring the complexity of the password that will be generated.

Check Logged In- Checks the current logged in state of the device where the Runtime Resource is running.

Login - Instructs a Login Agent Runtime Resource to retrieve a credential and execute a login.

Logout- Instructs a RPA Runtime resource to close all programs in the user session and logout of Windows. An optional delay can be passed in as the parameter 'Delay' which will hold off from logging out for the time specified. The process will still complete immediately, and the session will log out after the delay has passed.

Synaptein Proprietary

User Access Control (UAC) & Environmental Context

Fully customizable role-based access is available, using the Principle of Least Privilege. Individual users and whole groups of users can be assigned administrator-configurable combinations of system access rights.
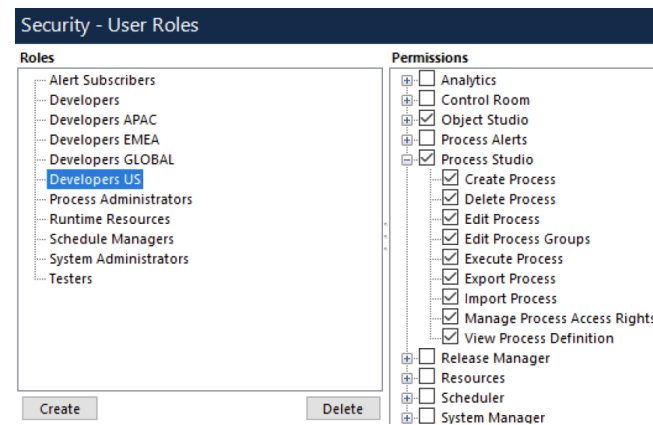

This access is defined separately within the context of each environment: Development, UAT and Production so that, for example, wholesale editing rights need not be granted across the board but instead in strict isolation.

User Access can also be governed centrally by means of integration with Microsoft Active Directory. This allows system access to be maintained under the central control and governance of an authorised administrator, in the context of users' other access rights across the network.

Multi-Team Environments

Multi-Team Environments enable organizations to model increasingly complex security configurations within RPA by extending the existing role-based access controls to enable more granular configurations.
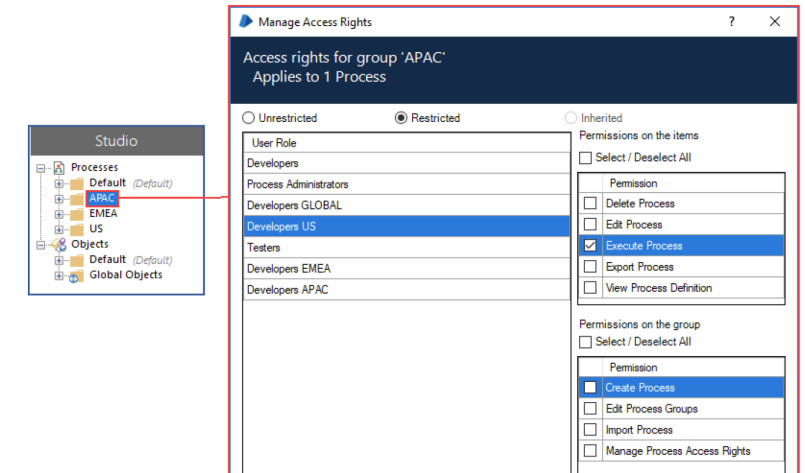
These capabilities better enable organizations to share RPA assets, such as Business Objects and Runtime Resources, with multiple teams within a given RPA environment by allowing permissions to be assigned, not only based on the type of asset, but also based on the hierarchical structure of the assets.

Compliance

Cradle-to-grave object & process change history, visual side-by-side process history comparison, real-time entity-level session logging, system audits, process execution audits, work queue snapshots, password protected exception screen capture, and integrated release management

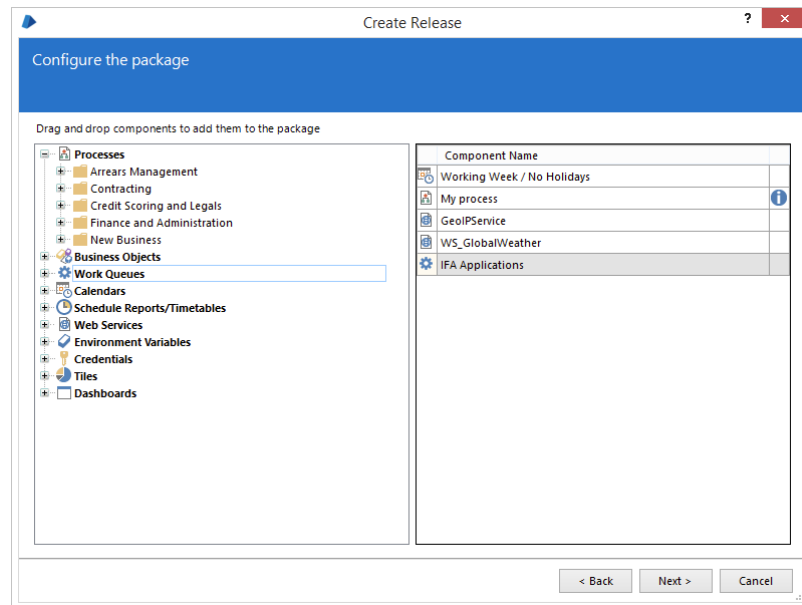# Process Change Audit

Process Version Comparison
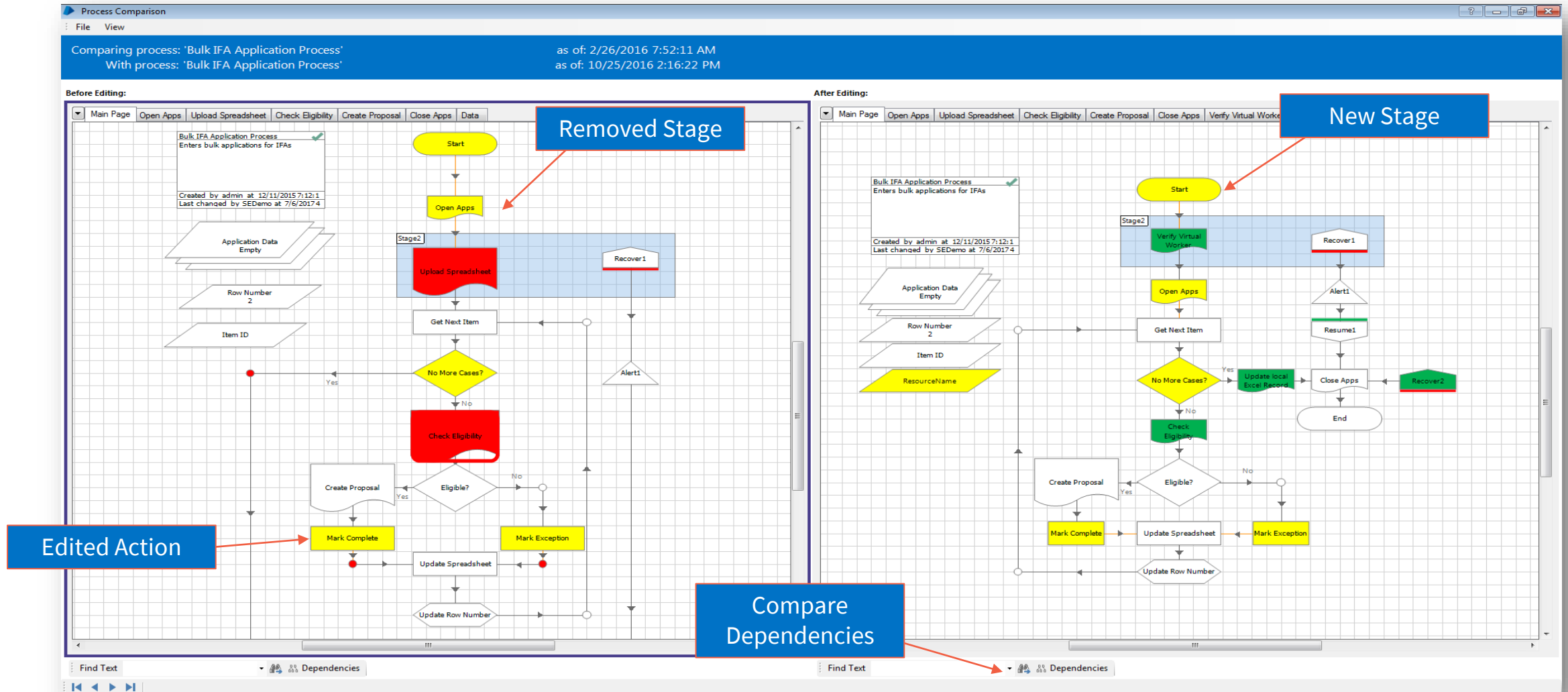
Change Management & Version Control

Release Manager

The RPA Release Manager provides a secure, audited and managed means of deploying changes from one environment to another – eg. From Development to Test & Production environments.

The Release Manager takes the form of an intelligent wizard that helps the user to wrap all of the components and dependencies of an automation into a single unit, allowing changes to be implemented atomically.

The resulting package is exported in an open xml-based file format which can be stored and versioned in independent repositories, if required.

Process Change and Version Control

Users are required to document their changes each time they save a change to a process and a full version history is captured along with the date/time and identity of the person making each change.

A full visual comparison can be made between any two versions in "Process History" and this uses a red / amber / green convention to highlight any deleted / modified / new stages, respectively.
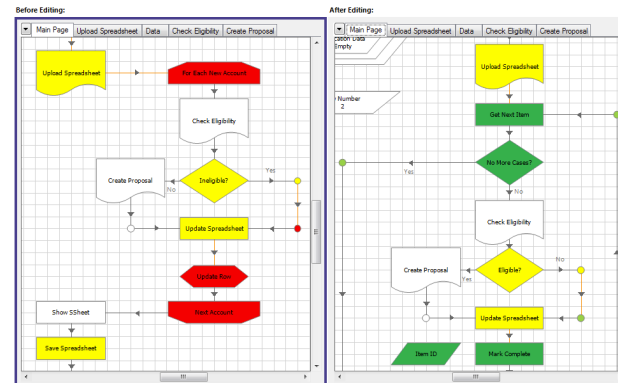
Process History exists not only as an audit feature but also to facilitate rollback to old versions and in order to facilitate the correct interpretation of historic log files against the corresponding process, as it appeared at the time.
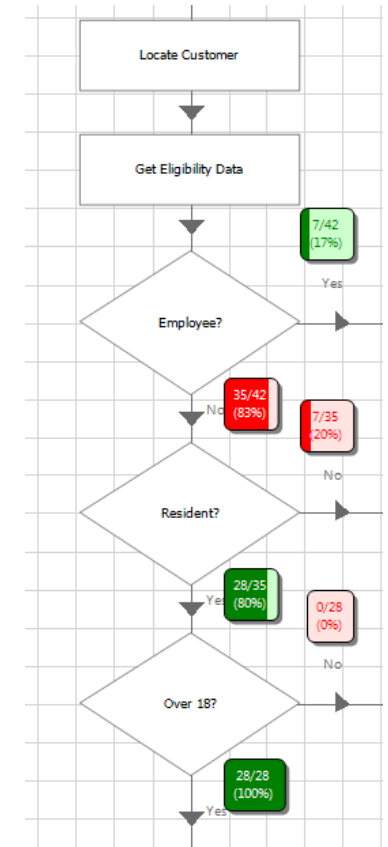
Platform & Process Audit

Changes to the platform itself are audited as well as changes within it. Each *event*, as well as each *change*, is audited.

"In effect, the System Administrator's behaviour is subject to the same level of scrutiny as that of ordinary users."

Events include actions such as merely logging in to the system; for example. *Changes* include interventions such as amending environment variables; making changes to users' privileges; the importing and exporting of data; etc.

In effect, this means that the System Administrator's behaviour is subject to the same level of scrutiny as that of ordinary users.

Operational Audit: Process Logs

Work items are typically captured in an RPA queue. This provides Operations teams with immediate access to case status and outcomes as well as management information on case times, creation & completion dates, etc.

A detailed history of activity is captured by runtime robots on a case by case basis, who record all of their activity in a session log. This record includes - for example - every button pressed, every piece of data that is read, every decision made, etc.

Where sensitive data is concerned, the logged information can be masked or omitted if necessary in order to comply with data standards such as PCI. The detail of the log relates directly back to the structure of the process diagram, making it easy to interpret for business users.

Log Contents

System Usage
- Login attempts, both successful & failed
- User activities, locations and outcomes

Administration
- Changes to system configuration
- User Management – deletions, additions, amendments
- Changes to endpoints, input/output locations, environment variables, etc.

Development Lifecycle
- Creation of new processes
- Process Changes – prominent audit trail and ability to provide peer review
- Change management – publication, import / export, migration, etc.

Operations
- Which user has started which process
- Where and when a process has executed and how long for
- Complete record of robot activities

Extensibility

Process Discovery Tool, Public & Private Digital Exchange, API Configurator, Data Gateways, Drag & Drop IA Skills Toolbar, & Intelligent Document Processing (Decipher Beta)

Process Discovery Tool

Group-Based Access

Inventory Management

Process Assessment
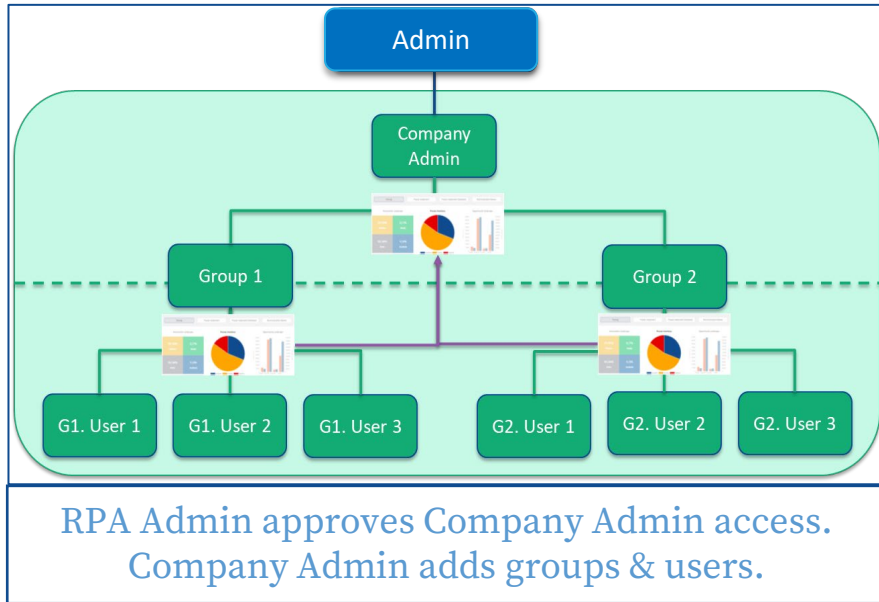
- Structure the Tool to reflect the organization & autonomously control User access.
- Drives engagement whilst maintaining centralised governance.
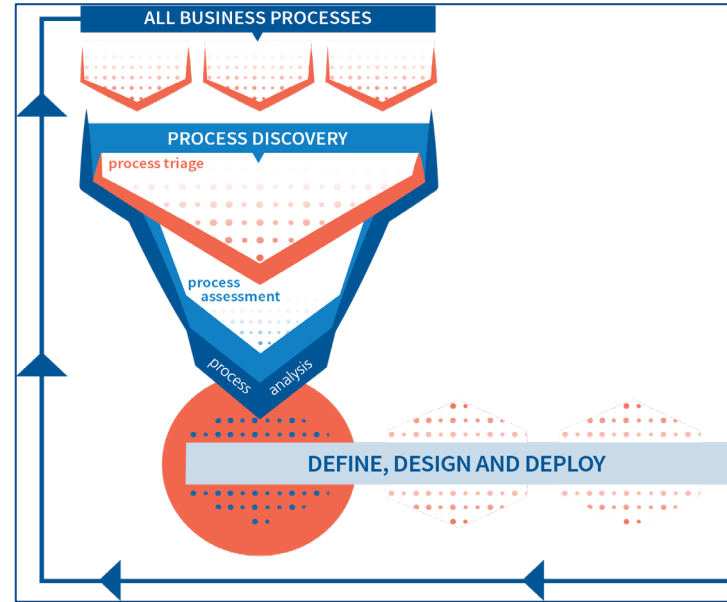
- Create a unique record of, & track, every process assessed.
- Enables progress tracking & benefit realisation calculation
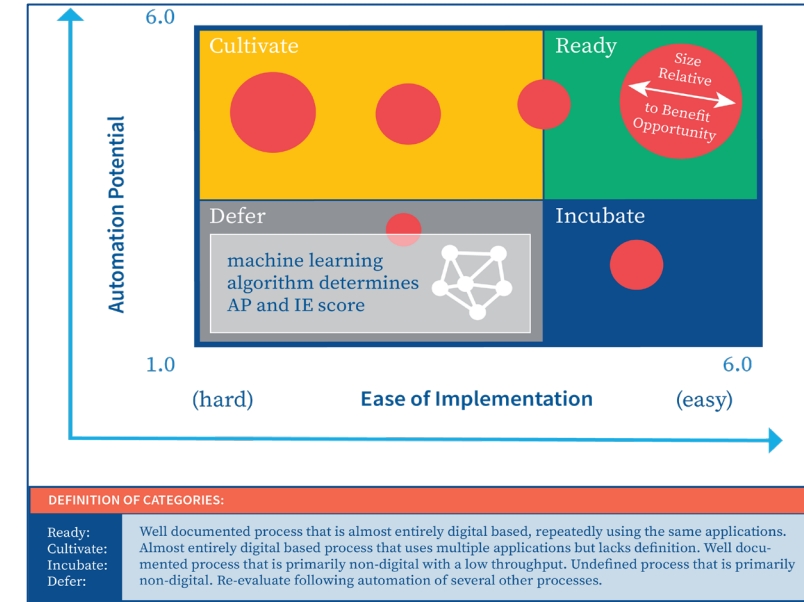
- Determine readiness for automation & relative benefit opportunity
- Facilitates decision making & management reporting

IA Skills & The Digital Exchange
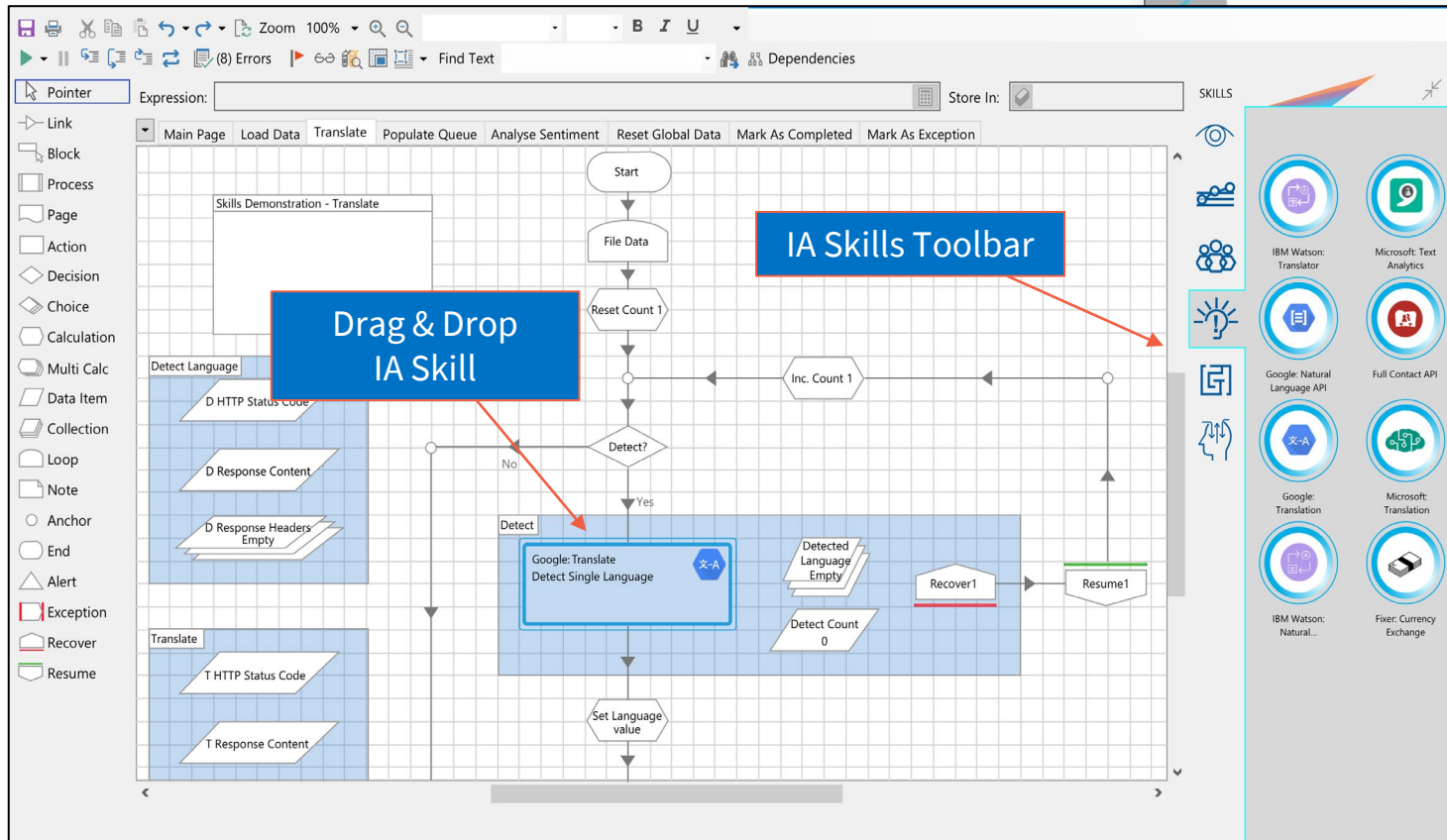
IA Skills Toolbar

Drag & Drop
IA Skill

Digital Workers - operating a process

Application Server

Data Gateway Engine

SQL DB

HTTP End-point

3rd Party DB

Flat File (Excel/CSV)

...Or custom
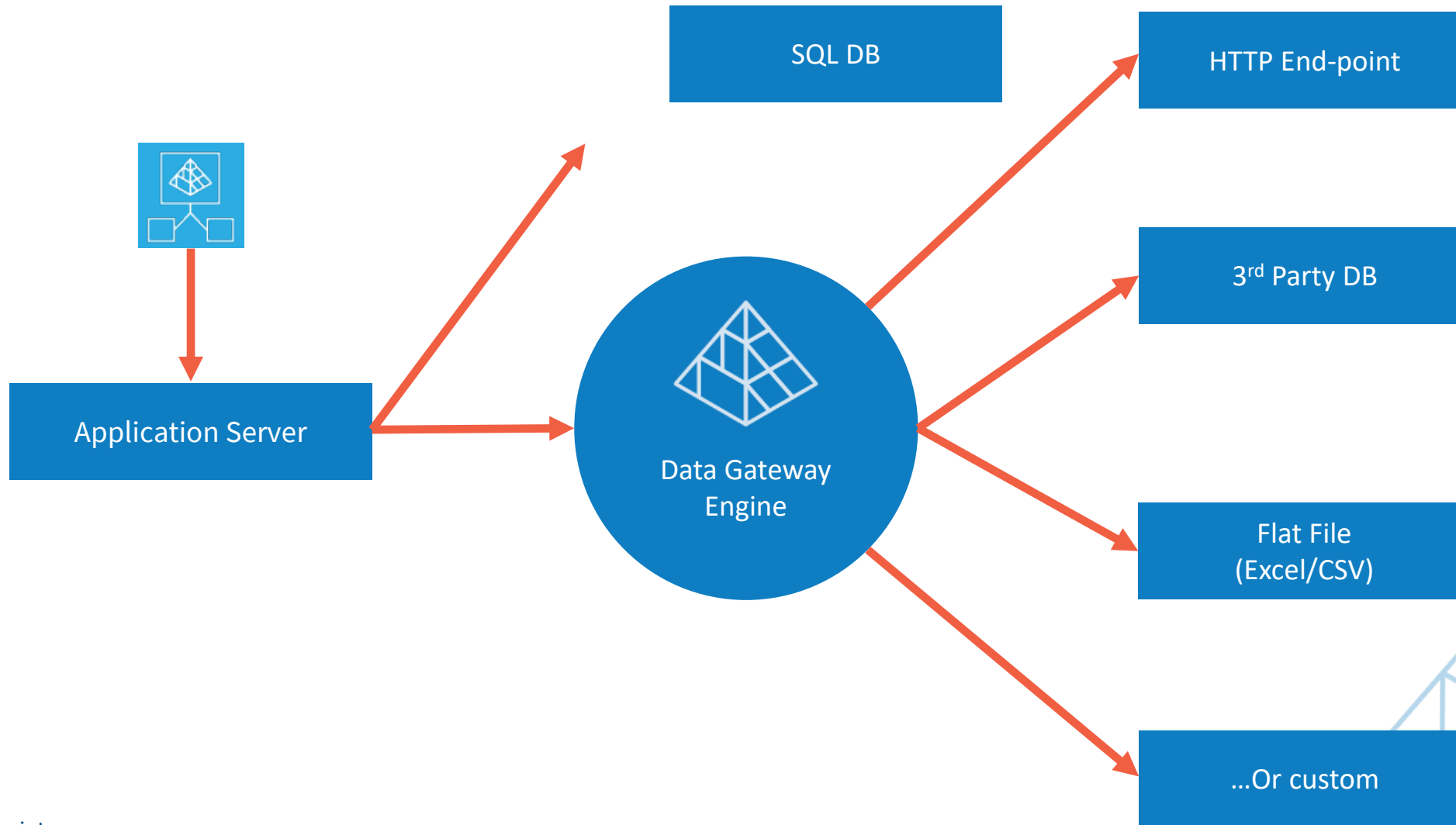
Key Technical Areas Summary

Scalability

- Fully centralized command & control
- Centrally updated re-usable objects
- Drag & drop design ('Plain English development')
- Expression builder with built-in debugging
- Automatic process design error check
- Dynamic work queue management, and many-to-many robot / process assignment

Resilience

- Intelligent tracking of underlying application logic
- Real-time logging to a central database (facilitates rollback, hot-failover, and disaster recovery)
- No license cost for Disaster Recovery
- Support for hybrid-cloud infrastructure (With reference architectures & build support from Professional Services)

Security

- FIPS 140-2 compliant
- Compliant with ICAM guidance from OMB Memorandum M-19-17 (NPE identity management – Digital Workers have their own identities)
- Robust support for Privileged Account Management solutions: AD/LDAP/CyberArk
- Encryption of data in transit and at rest
- No logging on local file system (logs encrypted in database)
- Business-level segregation of object and process permissions
- Decoupled build & run via granular roles-based access control (RBAC)
- Integrated encrypted password vault
- Data masking

Compliance

- Cradle-to-grave object & process change history
- Visual side-by-side process history comparison
- Real-time entity-level session logging (Both humans and Digital Workers)
- All aspects of the platform are auditable: System, Process Execution, etc
- Encrypted exception screen capture
- No shared user credentials or desktops between humans and Digital Workers

Extensibility

- Process Discovery Tool – Helps organizations quickly identify prime candidates for automation
- Public & Private Digital Exchange – download reusable objects developed by world-class technology alliance partners
- API Configurator
- Data Gateways – easy enhanced analytics output
- Drag & Drop Intelligent Automation Skills
- AI-powered Intelligent Document

Contact:

Sharad Dayma – CEO

sharad.d@synapone.com

703-209-2350