AUTOMATION ANYWHERE

الأمان المقدم على مستوى المؤسسات لتقنية التشغيل الآلي للعمليات الروبوتية

مقدمة

لماذا، و بعد مرور أكثر من 20 عامًا من الاستثمار في تقنيات التشغيل الآلي للعمليات التجارية، تم تشغيل أقل من 20% فقط من المهام آليًا؟ يكمن السبب الرئيسي في الافتقار إلى واجهات لبرمجة التطبيقات محددة جيدًا في 85% من أنظمة المؤسسات. وبالتالي، ينتج عن ذلك تراكمات متزايدة باستمرار من أعمال تقنية المعلومات المتعلقة بطلبات التكامل الصادرة من مجموعة من الأعمال التجارية.

لقد نشأت تقنية التشغيل الآلي للعمليات الروبوتية (RPA) برؤية تصبو نحو تمكين المستخدمين التجاريين من إنشاء روبوتات برمجية تستطيع التفاعل مع أنظمة المؤسسات، تمامًا مثل البشر. وبإمكان الروبوتات التي تعمل بتقنية RPA تسجيل الدخول إلى تطبيقات المؤسسات باستخدام بيانات اعتماد، تمامًا مثل البشر، وتشغيل المهام المنطوية على أي تطبيق للمؤسسة آليًا، بما فيها التطبيقات القديمة التي لا تحتوي على واجهات لبرمجة التطبيقات. إن معالجة الدعاوي، ومعالجة القروض، وتسوية الحسابات، وإصدار/إرسال الفواتير، وإصدار التقارير ما هي إلا أمثلة قليلة لعمليات التشغيل الآلي الممكنة التي يتم إجراؤها بين مختلف التخصصات التجارية.

من السهل رؤية إمكانية التوفير الكبير في الوقت والتكاليف، وزيادة رضا العملاء، وارتفاع المعنويات بين القوى العاملة، والقدرة على التمتع بأفضلية رائدة على المنافسين باستخدام تقنية RPA. وبرغم ذلك، فإن تحقيق هذه المكاسب بشكل كامل يعتمد على التميز بأحد الحلول على مستوى المؤسسات.

تتمثل بعض معايير التشغيل الآلي الضرورية في تقديم فعالية راسخة، وقابلية للتوسع، ومجموعة واسعة من الميزات التي ترفع من مستويات قابلية التطبيق وسهولة الاستخدام. ولكن هذه العناصر لا تشمل أكثر المتطلبات أهمية في الأعمال التجارية وهو: الأمان الشامل. إن وجود بنية متينة للأمان تتمتع بميزات تتيح توفير الدعم الكامل للمبادئ الأساسية، مثل أقل عدد من الصلاحيات وفصل المهام، مع تقديم حماية من البداية حتى النهاية لما يتم تضمينه من تطبيقات بالغة الأهمية وبيانات حساسة، يُعد ضروريًا لإتمام المهام.

يقدم هذا المستند نظرة عامة على أعلى معايير المجال لتوفير الأمان من فئة المؤسسات كما توضحه منصة القوى العاملة الرقمية الرائدة في السوق Automation Anywhere Enterprise.

من السهل رؤية إمكانية التوفير الكبير في الوقت والتكاليف، وزيادة رضا العملاء، وارتفاع المعنويات بين القوى العاملة، والقدرة على التمتع بأفضلية رائدة على المنافسين باستخدام تقنية RPA. وبرغم ذلك، فإن تحقيق هذه المكاسب بشكل كامل يعتمد على التميز بأحد الحلول على مستوى المؤسسات.

البنية والعمليات

إن استيعاب عناصر التحكم في الأمان اللازمة لتطبيق تقنية RPA على مستوى المؤسسات يعتمد على استيعاب المكونات التي يتألف منها الحل والعمليات المتعلقة بها.

المكونات الأساسية

كما هو موضح في **الشكل 1**، فإن ركائز البناء الأساسية لمنصة Automation Anywhere Enterprise تتمثل في غرفة التحكم ومنتجي الروبوتات ومشغلي الروبوتات.

غرفة التحكم

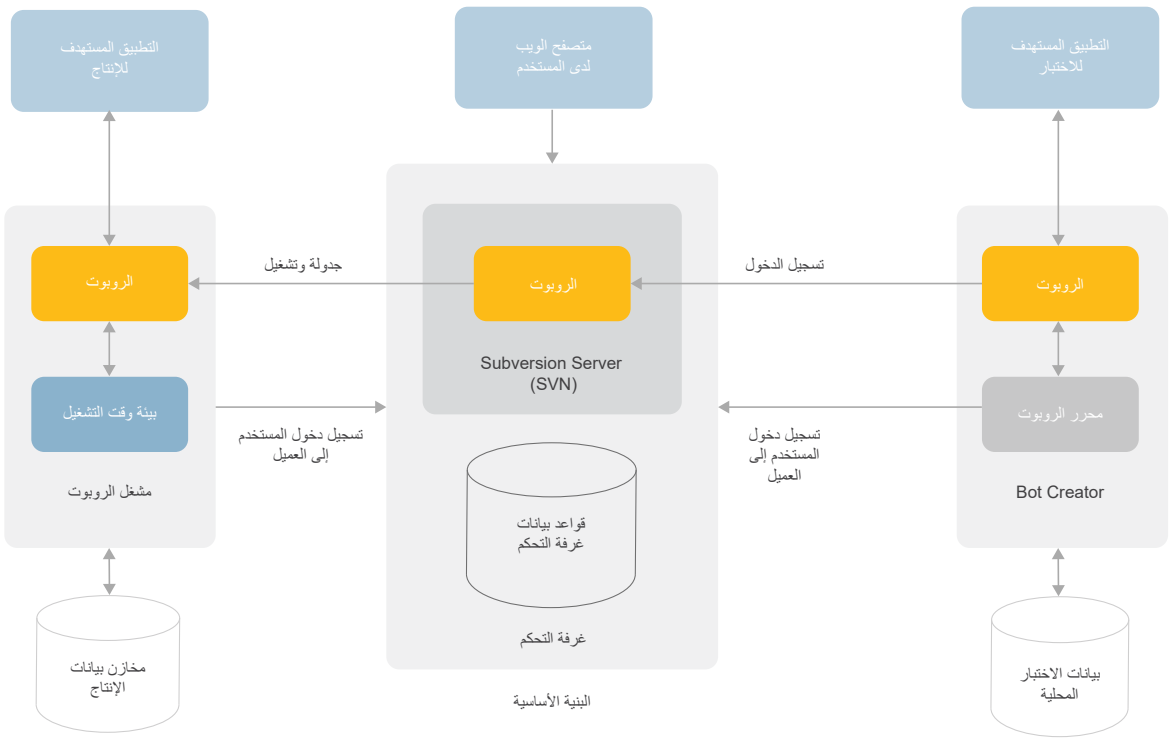
تعمل غرفة التحكم بمثابة العقل المدبر لبيئة التشغيل الآلي. فهي نظام إدارة يستند إلى نظام التشغيل Windows server تحتوي على قاعدة بيانات تكاملية توفر صورة موحدة للإدارة الكلية للنظام. كما تمثل غرفة التحكم أيضًا الوجهة التي يذهب إليها مسؤولو تشغيل RPA من أجل تنسيق أعمال القوى العاملة الرقمية، أي من أجل جدولة عملية تشغيل الروبوتات في المؤسسات، ونشرها، وتنفيذها، ومراقبتها، وإدارتها. وبالإضافة إلى ذلك، فإن ميزات التحكم المدمجة في الإصدار (Apache Subversion Server) تسهّل من التعاون بين عدة مستخدمين مع تنفيذها أفضل الممارسات لإدارة التغيير وإنشائها مستودعًا مركزيًا للروبوتات الجاهزة للإنتاج.

Bot Creator

يُستخدم Bot Creator في إنشاء روبوتات. وهو تطبيق يعمل على أجهزة سطح المكتب بنظام التشغيل Windows و يعمل على مستوى محطات العمل أو الأجهزة الافتراضية، كما أن خبراء عمليات الأعمال يستخدمون Bot Creator لإنشاء عمليات التشغيل الآلي لديهم واختبارها. يتم إنتاج الروبوتات باستخدام مُحرر الروبوت، بينما يعمل مشغل الروبوت على التسهيل من إجراء اختبارات على الروبوتات، باستخدام مثيلات للتطبيقات وبيانات اختبار محلية غير مخصصة للإنتاج. وبعد نجاح الروبوتات في الاختبار (مثل اختبار أدائها، وسلامة بياناتها، وأمنها)، يتم تسجيل دخولها في مستودع غرفة التحكم ليصبح نشرها متاحًا للإنتاج.

مشغل الروبوت

يعمل مشغل الروبوت على تشغيل الروبوتات. حيث يتولى مشغل الروبوت تشغيل الروبوتات في بيئة الإنتاج باستخدام رمز التطبيقات ذاته الذي يستخدمه Bot Creator، ولكن مع اختلاف مفتاح الترخيص، أي أنه يستخدم مثيلات الإنتاج للتطبيق المستهدف ومخازن بيانات الإنتاج. وفي الواقع، كل ما يستطيع مشغلو الروبوتات فعله هو تشغيل الروبوتات، نظرًا لعدم إتاحة وظيفتي الإنتاج والتحرير لهم. ويتم أيضًا دعم إمكانية تجميع مشغلي الروبوتات لإجراء العمليات بفعالية عالية وعلى نطاق واسع.



الشكل 1: البنية الأساسية لمنصة Automation Anywhere Enterprise

مكونات إضافية على مستوى المؤسسات

عند التفكير في إجراء عمليات على نطاق واسع، يبرز حلان آخران مهمان متعلقان بتقنية RPA ويرتبطان بالمؤسسات التي تسعى لتنفيذ عمليات النشر على مستوى المؤسسات، وهما: توسيع النطاق عند الطلب ومنصة Bot Insight.

توسيع النطاق عند الطلب

تقدم منصة Automation Anywhere Enterprise تقنية RPA كخدمة، بالاستفادة من السحابة العامة Amazon Web Services (AWS)، إلى جانب جميع الإمكانيات المرتبطة بها، بما فيها المرونة في زيادة/تقليص نشاط الإنتاج، والقياس حسب الاستخدام، وقابلية التوسع الأفقي بشكل غير محدود، والمراقبة المستمرة مع إنشاء سجلات تدقيق لبنية مشغل الروبوت التحتية. وينتج عن ذلك قابلية عالية للوصول من نقاط توصيل متعددة تعمل على تعزيز الأداء القائم على اتفاقية مستوى الخدمة (SLA) واستمرارية الأعمال التجارية، حتى عند حدوث تقلبات هائلة في أعباء العمل المخصصة للتشغيل الآلي.

Bot Insight

تمثل منصة Bot Insight نظامًا فرعيًا متكاملاً تمامًا داخل غرفة التحكم، حيث تتولى إجراء تحليل في الوقت الفعلي لعمليات الروبوت وبيانات العمليات التجارية. وتعمل Bot Insight على إصدار لوحات معلومات تلقائيًا يمكن تخصيصها باستخدام خوارزميات متطورة يتفرد بها كل روبوت. كما أن المستوى التفصيلي الذي تقدمه منصة Bot Insight حسب سجلات الأحداث الدقيقة للغاية بشأن عمليات الروبوت يتيح الدقة في إصدار تنبيهات، والاكتشافات المخصصة، والتعمق في مستوى التفاصيل بشكل تفاعلي، والتحليل بتسلسل زمني، والتمتع برؤية شاملة حول العمليات التشغيلية/التجارية. وبالإضافة إلى ذلك، فإن جميع البيانات يمكن تصديرها للسجلات المتعلقة بإدارة المعلومات الأمنية والأحداث الأمنية (SIEM) لإجراء مزيد من التحليل والتحقق وإصدار مزيد من التقارير.

روبوتات على أرض الواقع: نوعان من عمليات التشغيل الآلي

هناك أمر أخير يلزم توضيحه قبل الشروع في تناول إمكانيات الأمان ذات المستوى العالي لمنصة Automation Anywhere Enterprise، وهو ما يتعلق بالنوعين الرئيسيين من عمليات التشغيل الآلي: خاضعة للإشراف وغير خاضعة للإشراف.

يتمثل التشغيل الآلي الخاضع لإشراف في الحالة التي يتم فيها تسجيل دخول المستخدم على جهاز مشغل الروبوت للإشراف و/أو دعم تشغيل الروبوت بشكل فعّال. وقد تعود أسباب وجود المستخدم إلى تأدية الروبوت وظيفة ذات نوع مجدٍ يساعد في أداء أعمال المستخدم أو إجراء الروبوت لعمل بشكل دفعات بحيث يتطلب إدخالاً دوريًا أو التوجيه الظرفي من المستخدم. كما أن عمليات التشغيل الآلي الخاضعة لإشراف يُشار إليها أيضًا باسم عمليات التشغيل الآلي للمكاتب الأمامية.

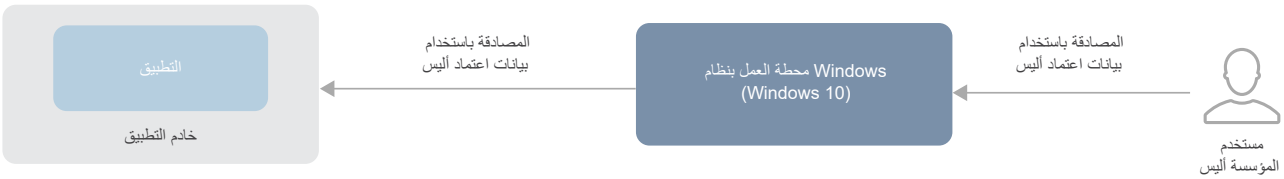
أما بالنسبة لعمليات التشغيل الآلي غير الخاضعة لإشراف، فإنها، كما يتضح من اسمها، تعمل بدون الحاجة لتفاعل المستخدم التجاري أو المشغل. ومن يتولى إجراء عمليات التشغيل الآلي غير الخاضعة لإشراف، يكون عادةً أحد المشغلين الذين لا يتوفر لديهم سوى القليل من المعرفة بشأن الروبوت أو التطبيق الذي يتم تشغيله آليًا أو غرض التشغيل الآلي. ويعمل المشغل بالاشتراك مع وحدة الأعمال على جدولة الروبوتات لتشغيلها على مشغلي الروبوتات. وأثناء عملية التشغيل، يراقب المشغل النواحي التشغيلية للروبوتات قيد التشغيل، مثل وحدة المعالجة المركزية (CPU) والذاكرة ومدى استخدام السعة التخزينية لضمان تشغيلها دون حدوث أخطاء أو استثناءات. أما لوحات المعلومات في غرفة التحكم، فتعرض جميع التفاصيل التشغيلية للروبوتات أثناء بقائها قيد التشغيل. وفي حالة عدم اكتمال أية عملية تشغيل آلي بدون إشراف بسبب حدوث خطأ، قد يطبّق المشغل إجراءات لإصلاح عملية التشغيل الآلي وإعادة تشغيلها، أو يُصعّد الأمر إلى فريق RPA أو وحدة الأعمال لتشخيص المشكلة وإصلاحها.

عملية تحديد الهوية والمصادقة متعددة الطبقات لتحقيق الأمان متعدد الطبقات في منصة RPA للمؤسسات

هناك مبدأ أساسي تقوم عليه بنية الأمان لمنصة Automation Anywhere Enterprise يتمثل في عدم السماح بإمكانية الوصول أو اتخاذ إجراء دون الحصول على مصادقة مسبقة للكيان المعني. ويسري هذا الأمر على البشر والروبوتات على حد سواء. ومن ثمّ توجد عملية مصادقة متعددة الطبقات لعمليتي التشغيل الآلي الخاضعة للإشراف وغير الخاضعة للإشراف.

التعرّف على هوية الأشخاص وأدوارهم: عمليات المصادقة النموذجية في المؤسسات

يمكن التعامل مع بيانات الاعتماد والشخصيات من خلال طبقات متعددة. جرّب التفكير في سيناريو بسيط لعملية مصادقة تتم في مؤسسة (انظر **الشكل 2**). تُجري أليس، وهي من ضمن المستخدمين بالمؤسسة، المصادقة للوصول إلى محطة العمل لديها التي تعمل بنظام Windows. ومن ثم، تبادر أليس بتسجيل الدخول إلى أحد التطبيقات التي تعمل عن بعد، حيث تُجري عملية المصادقة عبر استخدام بيانات الدخول إلى خدمة Active Directory في شبكة Windows Domain أو ربما عبر بروتوكول Kerberos حسب مدى حصول محطة العمل لديها على تذكرة صالحة. في هذا السيناريو، تتضمن سلسلة المصادقة شخصًا واحدًا مع بيانات اعتماده.

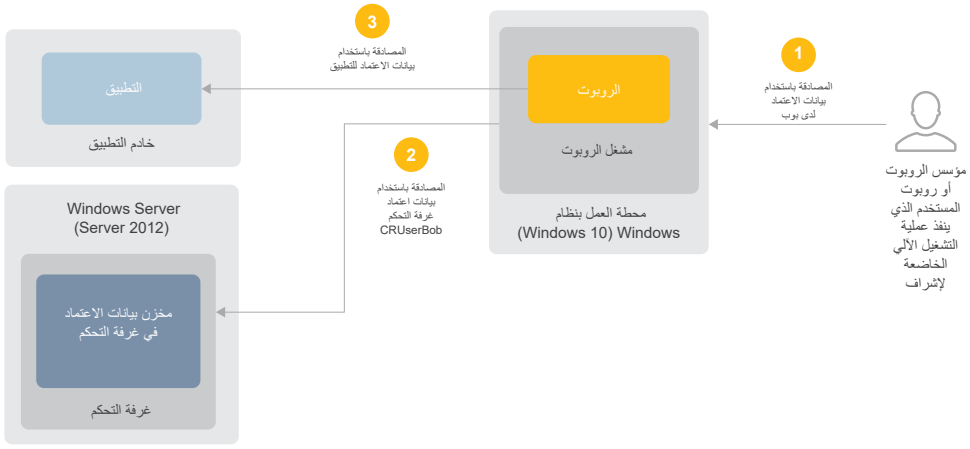


الشكل 2: عملية المصادقة النموذجية في المؤسسات

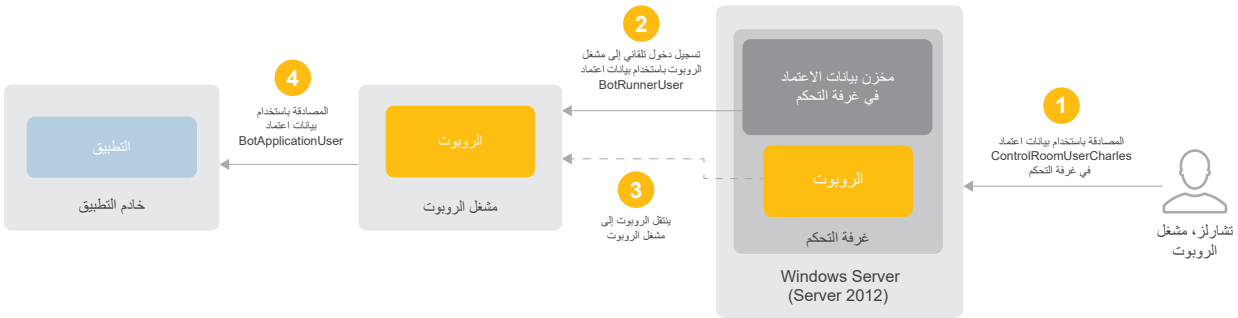
الآن، انظر في السيناريو المتعلق بالتشغيل الآلي الخاضع لإشراف الموضح في **الشكل 3**. في هذه الحالة، يعكف المستخدم، بوب، على اختبار أحد الروبوتات أو تشغيل عملية تشغيل آلي خاضعة لإشراف كجزء من يومه المعتاد في العمل. في الخطوة رقم 1، يُجري المصادقة للوصول إلى محطة عمل مشغل الروبوت باستخدام بيانات اعتماده الشخصية (تمامًا مثلما حدث في سيناريو أليس بالأعلى). وفي الخطوة رقم 2، يتولى تشغيل عميل Automation Anywhere Enterprise وإدخال مُعرف المستخدم وكلمة المرور لديه في غرفة التحكم، مما يؤدي إلى مصادقة برنامج العميل للوصول إلى غرفة التحكم. وفي الخطوة رقم 3، يشغّل الروبوت الذي يتمكن، بدوره، من الوصول إلى تطبيق يتطلب إجراء مصادقة. إن بيانات الاعتماد التي استخدمها الروبوت في هذه الخطوة يمكن تخزينها في برنامج Enterprise Credential Vault واستعادتها من قِبل الروبوت أثناء وقت التشغيل، أو قد تتوفر وسيلة لاجتياز طلب بيانات الاعتماد الشخصية لبوب (وفقًا للحيز المتاح في محطة العمل لديه وخادم التطبيق الموجود في المجال ذاته). وفي كلتا الحالتين، ستتمثل النتيجة إجمالاً في توفير ثلاث طبقات من تحديد الهوية وعملية المصادقة.

توجد ثلاث طبقات من عملية المصادقة تم استخدامها في سيناريو التشغيل الآلي غير الخاضع لإشراف المبين في **الشكل 4**، وإن كانت هناك بعض التغييرات. في هذه الحالة، يبدأ المستخدم، تشارلز، بإجراء المصادقة للوصول إلى غرفة التحكم حتى يتمكن من تحديد أحد الروبوتات اللازم تشغيله، وذلك إما على الفور أو في وقت مجدول.

في الخطوة رقم 2، عندما يبدأ الوقت المخصص لتشغيل الروبوت، تباشر غرفة التحكم عملية تسجيل دخول تلقائي إلى محطة عمل مشغل الروبوت، باستخدام بيانات اعتماد BotRunnerUser. وبعد أن يتم تنزيل الروبوت في وظيفة Player (المشغّل) المحلية (الخطوة رقم 3) ويبدأ التشغيل، يتولى إجراء المصادقة للوصول إلى التطبيق المستهدف باستخدام بيانات اعتماد BotApplicationUser (الخطوة رقم 4). قد تكون بيانات اعتماد BotApplicationUser إحدى البيانات التي تم استردادها من مخزن بيانات الاعتماد أو قد تكون وسيلة لاجتياز طلب بيانات اعتماد BotRunnerUser، تمامًا مثل سيناريو التشغيل الآلي الخاضع لإشراف.



الشكل 3: عملية المصادقة المتعلقة بسيناريو التشغيل الآلي الخاضع لإشراف



الشكل 4: عملية المصادقة المتعلقة بسيناريو التشغيل الآلي غير الخاضع لإشراف

خيارات المصادقة وعمليات التكامل لإدارة الهوية وإمكانية الوصول (IAM)

إن الخيارات المدعومة لعملية المصادقة في غرفة التحكم تشمل خدمة Active Directory باستخدام بروتوكول النفاذ إلى الدليل البسيط (LDAP)، وخدمة Active Directory باستخدام بروتوكول Kerberos، والمصادقة المحلية باستخدام مخزن بيانات الاعتماد المضمن (سيتم التحدث عنه في قسم لاحق).

أما الخيارات الأخرى لإدارة الهوية وإمكانية الوصول التي تُتاح لعمليات النشر في المؤسسات، فتشمل ما يلي:

+ دعم تسجيل الدخول الأحادي استنادًا إلى الإصدار 2.0 من لغة ترميز التأكيدات الأمنية (SAML 2.0)
+ التكامل مع حلول إدارة بيانات الاعتماد/الوصول المتميز التابعة لأطراف خارجية (مثل CyberArk وOne Identity وThycotic)

التحكم في الوصول الشامل المستند إلى الأدوار

لا يشكّل نجاح عملية المصادقة إلا المستوى الأول من تطبيق التحكم في الوصول الإلزامي الذي توفره بنية الأمان لمنصة Automation Anywhere Enterprise. ويعادله في الأهمية دعم إمكانية التحكم في الوصول المستند إلى الأدوار أو RBAC والمميز بدقة بالغة، خاصة عندما يتعلق الأمر بالالتزام بالمبادئ الأساسية لأقل عدد من الصلاحيات وفصل المهام.

هناك خمسة أدوار مختلفة (انظر **الجدول 1**) يلزم أخذها بعين الاعتبار ضمن البنية الأساسية والوظائف الرئيسية لمنصة RPA. يستخدم صانعو الروبوتات Bot Creator لالتقاط القواعد المنطقية للأعمال وإنشاء عمليات تشغيل آلي مناظرة. ويعمل صانعو الروبوتات بجانب التطبيقات الاختبارية ومجموعات البيانات حتى لا تتأثر أنظمة الإنتاج أثناء مرحلة التطوير. وسيخضع أي روبوت بمفرده إلى العديد من أعمال التكرار والإصدارات المختلفة بشكل نموذجي، وذلك ليس أثناء مرحلة التطوير الأولي فقط، لكن عندما يتم أيضًا تحديث العمليات التجارية المرتبطة و/أو التطبيق المستهدف في أي وقت. كما يعمل مختبِرو الروبوتات أيضًا برفقة Bot Creator لاختبار أداء الروبوتات وسلامة بياناتها وأمنها، مع التأكد من تولي كل روبوت المهمة المخصصة له بطريقة آمنة. ويُعد مختبِرو الروبوتات بمثابة المرحلة الثانية من عملية المصادقة التي يخضع لها الروبوت قبل التمكن من تشغيله من خلال بيانات الإنتاج وتطبيقاته.

الدور	الوصف
مسؤول RPA	(مسؤول عن إدارة النظام) تهيئة المكونات والأدوار والواجهات
صانع الروبوت	خبير في مجال عمليات الأعمال يتولى إنشاء الروبوتات باستخدام محرر المهام ويُجري الاختبارات الوظيفية الأساسية
مختبِر الروبوت	مختبِر لضمان الجودة يفحص الروبوتات للتأكد من دقتها الوظيفية وأدائها وأمنها
معزز الروبوت	مسؤول يمنح الموافقة على الروبوتات وينقلها بين مراحل التطوير والاختبار والإنتاج
مسؤول تشغيل RPA	مشغل يتولى جدولة الروبوتات وتشغيلها ومراقبة أدائها

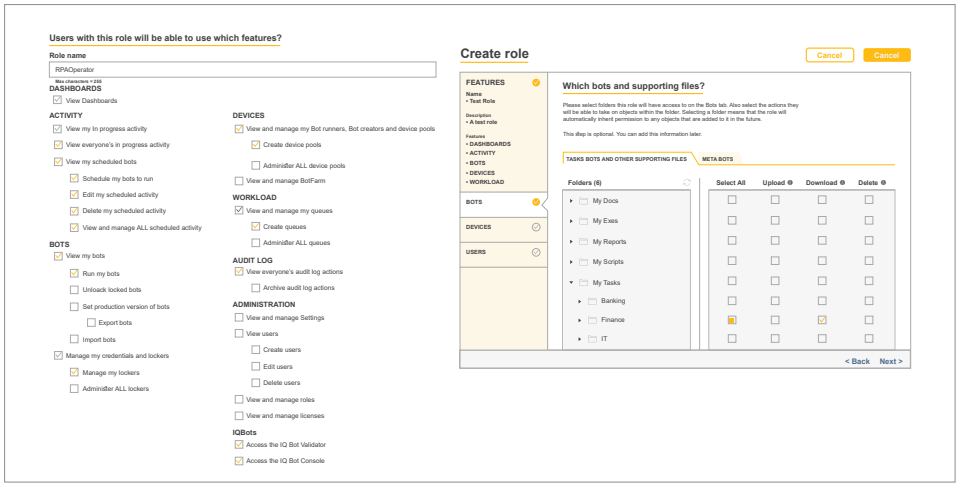
الجدول 1: أدوار RPA الرئيسية في منصة Automation Anywhere Enterprise

بمجرد اختبار أي روبوت وخضوعه لفحص أمني، يعمل معزز الروبوت برفقة صانعي الروبوتات/مختبِر الروبوت لتحديد نوع الإصدار للروبوت الذي ينبغي استخدامه في عملية الإنتاج. حيث يعد ذلك بمثابة الإصدار الوحيد للروبوت الذي سيكون ظاهرًا أمام مسؤول تشغيل الروبوت الذي يتولى أعمال التنسيق مع وحدة/وحدات الأعمال من أجل جدولة الروبوت وتشغيله. كما يتولى مسؤول تشغيل الروبوت المسؤولية أيضًا عن مراقبة أداء الروبوت داخل غرفة التحكم، بما في ذلك استكشاف أية مشكلات ظاهرة أثناء وقت التشغيل وإصلاحها. وأخيرًا، فإن مسؤولية الإدارة الكلية للمنصة، بما في ذلك تهيئة المكونات والواجهات وجميع الأدوار/الأذونات، تقع على عاتق مسؤول RPA.

الفصل المتطور للمهام

تمثل هذه المجموعة الجوهرية من الأدوار نقطة بداية أساسية لعناصر التحكم في الوصول المستند إلى الأدوار (RBAC)، ولكن يمكن أيضًا فصل المهام بقدر أكبر داخل منصة Automation Anywhere Enterprise. فباستخدام معالج إنشاء الأدوار المضمن، يستطيع المسؤولون بسهولة تحديد أدوار مخصصة وصلاحيات/أذونات للإعدادات بحيث تستأثر بالمجموعة الكاملة للعناصر والوظائف في غرفة التحكم، بما فيها إدارة المستخدم، والترخيص، ومخزن بيانات الاعتماد، ومجموعة مشغلي الروبوتات، والجداول الزمنية للروبوتات، والعمليات/لوحات المعلومات المتعلقة بالروبوتات، وسجلات التدقيق. وأثناء تحديد كل صلاحية، سيضيف المعالج بشكل ديناميكي خطوات للحصول على صلاحيات عرضية/مستمدة.

على سبيل المثال، عند تحديد الصلاحيات BOTS (الروبوتات) > View my bots (عرض الروبوتات لدي) > Run My bots (تشغيل الروبوتات لدي) (انظر **الشكل 5**)، سيضيف سير العمل خطوة للإشارة إلى "Bot Folders" (مجلدات الروبوتات) المحددة (أي مجموعات الروبوتات) التي يتم منح إمكانية الوصول إليها. وستتمثل النتيجة النهائية في توفير القدرة على تأسيس أدوار تتطلب دقة عالية مع عناصر تحكم دقيق للغاية في الوصول تكفي لتلبية احتياجات البيئات الأكثر صرامة وأمانًا وخضوعًا للوائح الامتثال.



الشكل 5: إنشاء الأدوار مع تطبيق مصادقة دقيقة للغاية

مستويات تحكم مستقلة

إلى جانب إمكانات RBAC واسعة النطاق، تعمل منصة Automation Anywhere Enterprise بشكل أساسي على فصل المهام بصورة منطقية من خلال توظيف بنية تفصل بصورة كاملة بين مهام تطوير الروبوتات وتشغيل الروبوتات.

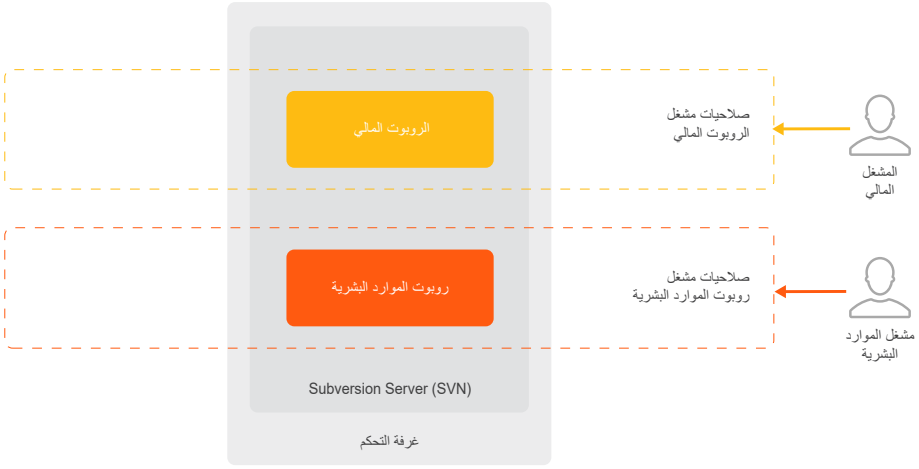
يمكن لمنتجي الروبوتات تحميل الروبوتات إلى نظام التحكم بالإصدار داخل غرفة التحكم وتنزيلها منه فقط. وفي الوقت ذاته، تقتصر مهام مُشغلي الروبوتات على تشغيل الروبوتات؛ وليس لديها إمكانية الوصول إلى وظيفة إنشاء الروبوتات واختبارها. يمثِّل فصل المهام هذا المُطبَّق من خلال البنية مصادقة مزدوجة متسقة مع أفضل ممارسات المعهد الوطني للمعايير والتقنية (NIST)، وذلك لأنه يتطلب بشكل أساسي (كحد أدنى) تمكين التشغيل الآلي للعمليات التجارية بواسطة المُطوِّر والمستخدم التجاري معًا.

مجالات معالجة مستقلة

إن حالة الاستخدام الفعال لإمكانات RBAC لدى المنصة، ولا سيما للمؤسسات الكبيرة، تتمثَّل في تأسيس مجالات معالجة مستقلة (انظر **الشكل 6**). ويمكن تحقيق ذلك من خلال تنظيم / تخزين الروبوتات على نحو مُحدَّد لكل مجال مطلوب في مجلد مناظر داخل غرفة التحكم.

وأحد الأمثلة على ذلك: يتم وضع الروبوتات المرتبطة بالتطبيقات المالية في مجلد الشؤون المالية، بينما يتم وضع الروبوتات المرتبطة بالموارد البشرية في مجلد الموارد البشرية. ومن ثَمَّ، تُخصَّص لمسؤولي تشغيل الروبوتات لدى قسم الشؤون المالية صلاحيات استخدام روبوتات الشؤون المالية ومشغلي الروبوتات للشؤون المالية فقط؛ بينما تُخصَّص لمسؤولي تشغيل الروبوتات لدى قسم الموارد البشرية صلاحيات استخدام الروبوتات ومشغلي الروبوتات لقسم الموارد البشرية فقط، وهكذا بالنسبة لباقي مجالات المعالجة / التشغيل الآلي (انظر **الشكل 6**).

والمحصلة النهائية هي مواصلة فصل المهام وعزل التطبيقات والبيانات المرتبطة—في هذا الوقت على مستوى المجال / OU (الوحدة التنظيمية)—وذلك لأن المشغلين الفرديين لن يتمكَّنوا من رؤية الروبوتات الموجودة خارج المجال المحدد لهم أو تشغيلها.



الشكل 6: دعم مجالات المعالجة المستقلة

حماية البيانات من البداية حتى النهاية

تُعد المصادقة متعددة الطبقات والتحكم الدقيق للغاية في الوصول أمرين مُهمّين لإيجاد بيئة تخضع لمُراقبَة مُحكمة. وكذلك حماية البيانات من البداية حتى النهاية، والتي تُعد ضرورية للحفاظ على سرية العمليات التجارية الحيوية والبيانات الحساسة والأسرار ذات الصلة (مثل بيانات الاعتماد) وسلامتها.

ومن ثمَّ تُلبّي منصة Automation Anywhere Enterprise هذه الحاجة من خلال تضمين مخزن بيانات الاعتماد، كما توفر مجموعة واسعة النطاق من وسائل الحماية والتي لن توفر الحماية للبيانات الخاملة والبيانات قيد النقل فحسب، بل أيضًا أثناء استخدامها على الأنظمة الفردية.

مفاتيح التشفير و مخزن بيانات الاعتماد

يعرض **الشكل 7** مفاتيح التشفير الرئيسية المستخدمة من خلال المنصة، بجانب علاقتها بمخزن بيانات الاعتماد. يتم التشفير بأكمله باستخدام وحدات تشفيرية صالحة للمستوى 1 المحدد بالمعيار FIPS 140-2.

أثناء التثبيت (الجزء الأيسر من **الشكل 7**، ينتج النظام مفتاحًا مزدوجًا عامًا / خاصًا بحجم 2048 بت بواسطة خوارزمية التشفير "RSA" ومفتاحًا بحجم 256 بت من خلال خوارزمية التشفير "AES". يُشار إلى المفتاح الخاص من زوج RSA 2048 بالمفتاح الرئيسي، بينما يُشار إلى مفتاح AES 256 بمفتاح البيانات. يُقدَّم المفتاح الرئيسي إلى مسؤول التثبيت لحفظه في موقع آمن ماديًا خارج النظام. بينما يُستخدم المفتاح العام لتشفير مفتاح البيانات. وبعد ذلك يتم تخزين كل من المفتاح العام ومفتاح البيانات المُشفّر في قاعدة البيانات. وعند الاستخدام، يتم وضع جميع المفاتيح والبيانات المُشفّرة في ذاكرة آمنة مُشفّرة باستخدام "Microsoft Data Protection API" (واجهة برمجة التطبيقات لحماية البيانات من Microsoft) (DPAPI).

أثناء بدء تشغيل غرفة التحكم أو إعادة تشغيلها (الجزء الأيمن من **الشكل 7**)، يُطلب من المسؤول تقديم المفتاح الرئيسي. تتم استعادة مفتاح البيانات المُشفّر من قاعدة البيانات ويتم فك تشفيره باستخدام المفتاح الرئيسي. أصبح الآن مفتاح البيانات جاهزًا للاستخدام. وعندما يعمل النظام على تخزين البيانات في مخزن بيانات الاعتماد واستعادتها منه، يتم استخدام مفتاح البيانات لتشفير البيانات وفك تشفيرها.

يُستخدم مخزن بيانات الاعتماد لتخزين جميع بيانات الاعتماد التي تتم إدارتها بالنظام والبيانات المهمة لتهيئة النظام. ويمكن استخدامه أيضًا لتخزين البيانات الحساسة الأخرى (مثل زوج الاسم-القيمة) المستخدمة في عمليات التشغيل الآلي المؤسسية. ونتيجة لذلك، يمكن لصانعي الروبوتات تجنب الممارسات غير الآمنة لإجراء الترميز المضمن لبيانات الاعتماد والبيانات / الوسيطات الحساسة الأخرى مباشرة داخل عمليات التشغيل الآلي.

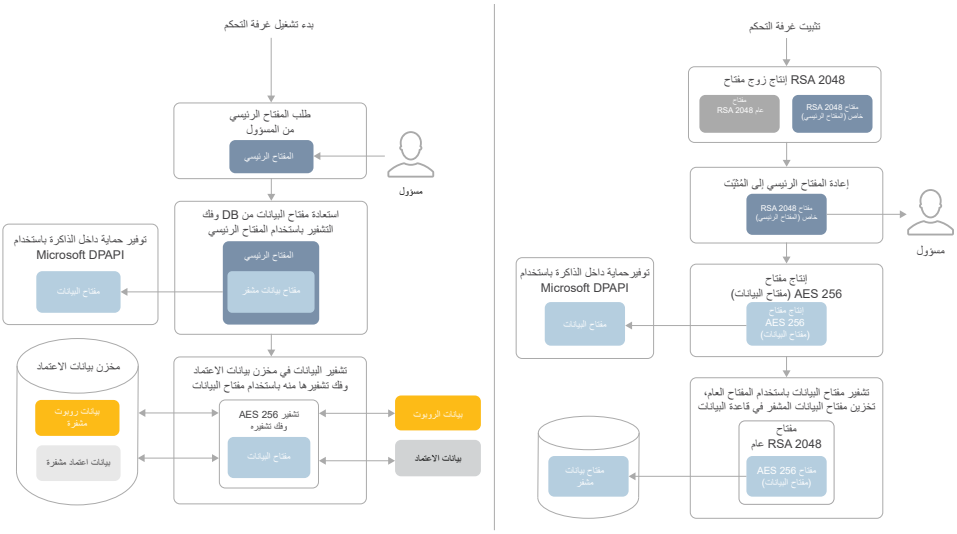
حماية البيانات الخاملة

بالإضافة إلى تشفير بيانات الاعتماد المحلية وتحديد بيانات وقت التشغيل المستخدمة بواسطة الروبوتات، يوفر مخزن بيانات الاعتماد تخزينًا آمنًا لمعلمات التهيئة الحساسة والتفاصيل المتعلقة بالخدمات التكاملية للبريد الإلكتروني والتحكم بالإصدار.

حماية البيانات قيد النقل

تستخدم جميع خدمات الشبكة الموجودة لدى العملاء وغرفة التحكم بروتوكول أمان طبقة النقل (TLS) الإصدار 1.2، لضمان أمن البيانات وسلامتها أثناء نقلها بين المكونات.

إن بيانات الاعتماد المستخدمة لمصادقة Bot Creator / مُشغِّل الروبوت للوصول إلى غرفة التحكم يتم تشفيرها قبل أن يتم إرسالها عبر اتصال TLS آمن. وهذه الطبقة الإضافية للتشفير لا توفر حماية ضد مشاكل مكدس الشبكة (مثل الثغرة الأمنية "Heartbleed" (هارت بليد) فحسب، بل تمنع أيضًا كشف بيانات اعتماد عمليات التنفيذ التي يتم فيها إنهاء اتصال TLS للطبقة الخارجية لدى موازن تحميل الواجهة الأمامية.



الشكل 7: بنية التشفير لمنصة Automation Anywhere Enterprise

حماية البيانات قيد الاستخدام

يبدأ تأمين وقت التشغيل بإجراء حماية من خلال توزيع بيانات الاعتماد. لا توجد، على وجه التحديد، سعة تخزينية محلية لبيانات الاعتماد على مُشغِّلي الروبوتات. إن بيانات الاعتماد والبيانات الأخرى التي تتم استعادتها بشكل ديناميكي من مخزن بيانات الاعتماد للاستخدام في عمليات التشغيل الآلي يتم الاحتفاظ بها بتنسيق مُشفَّر فقط في ذاكرة غير دائمة ويتم مسحها بمجرد انتهاء الروبوت ذي الصلة من العمل المُخصص له.

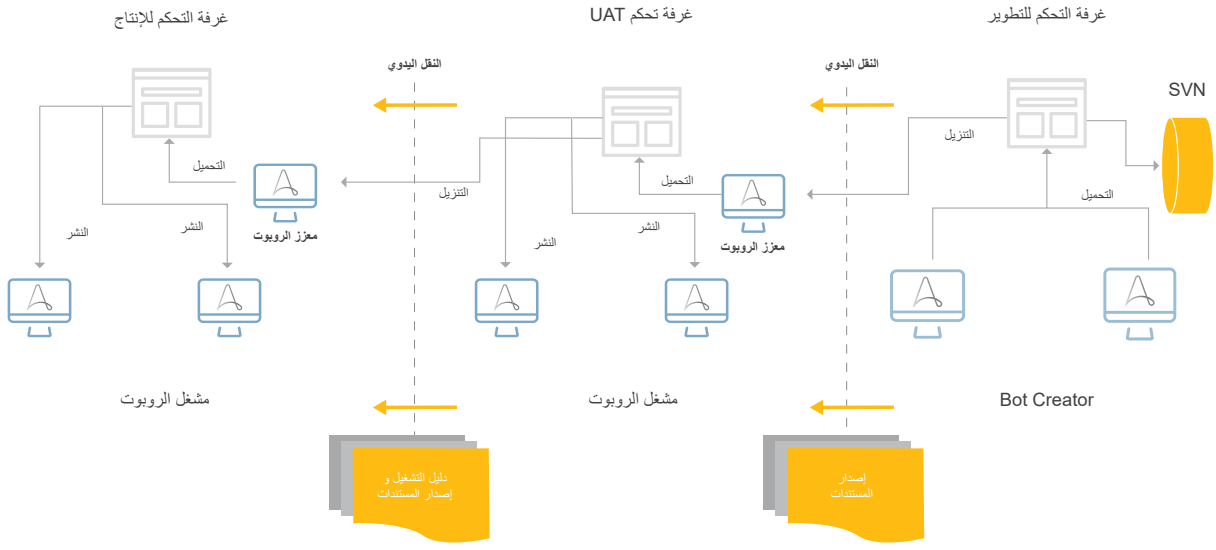
تتضمّن خيارات التهيئة والميزات الأخرى التي يمكن استخدامها لمنع الوصول غير المُصرَّح به إلى المعلومات السرية (مثل تسرُّب البيانات) أو التلاعب بالروبوتات أثناء وقت التشغيل ما يلي:

+ وضع التخفي – حيث لا يتم عرض نوافذ للبرامج على الشاشة المحلية ويكون لدى المستخدمين الذين سجَّلوا الدخول خيار تعطيل تسجيل الصور على منتجي الروبوتات ومُشغِّلي الروبوتات، وبذلك يتم منع تخزين المعلومات الحساسة المعروضة على الشاشة في الروبوتات
+ خيار تأمين الإدخال – يُتيح إمكانية تعطيل الماوس ولوحة المفاتيح بالجهاز الذي يتم إجراء التشغيل الآلي به
+ خيار الحد الزمني – يُتيح إمكانية تعيين حد زمني يتم بعده إنهاء التشغيل الآلي في حالة عدم اكتمال المهام المخصصة للتشغيل الآلي في الوقت المحدد لها
+ خيار التحكم المركزي – يُتيح إمكانية التحكم المركزي (مثل الإيقاف المؤقت والاستئناف والإيقاف) في تشغيل عمليات التشغيل الآلي التي يتم تشغيلها عن بُعد من داخل غرفة التحكم

دعم تأمين دورة حياة تطوير البرمجيات (SDLC)

لزيادة عناصر التحكم ووسائل الحماية المُطبّقة على بيئة التشغيل الآلي، يمكن "توسيع" سيناريو النشر الأساسي الموضح سابقًا من أجل تعزيز الوفاء بمتطلبات أفضل الممارسات لتأمين دورة حياة تطوير البرمجيات (SDLC)، كتلك المطلوبة من قِبل FISMA وFedRamp وPCI DSS. سيوفر نموذج النشر المتقدّم الناتج ثلاث مناطق RPA مختلفة – منطقة واحدة لكل من التطوير واختبار قبول المستخدم (UAT) والإنتاج (راجع الشكل 8). وكل منطقة يتم فصلها (عزلها) بشكل منطقي لدى مجموعات المستخدمين المختلفة التي لديها أدوار وصلاحيات مستقلة. تمثّل الخطوط الرأسية المتقطعة جدران الحماية وتقسيم الشبكة.

وكما هو الحال في نموذج النشر الأساسي، تبدأ دورة حياة الروبوت بالتطوير. وبمجرد اقتناع صانعي الروبوتات بالروبوت، يعمل معززو الروبوت لمنطقة UAT على نقل الروبوت من مستودع تعيين إصدار التطوير (SVN) إلى مستودع UAT. والغرض الوحيد من منطقة UAT هو اختبار دقة الروبوتات وأدائها وأمنها. وبمجرد اجتياز الروبوت اختبار القبول، يعمل معزز الروبوت لقسم الإنتاج على نقل الروبوت إلى منطقة الإنتاج. في هذه المرحلة، يكون الروبوت قد بلغ مرحلة الإنتاج وأصبح متاحًا للاستخدام مع تطبيقات الإنتاج لدى مسؤولي تشغيل RPA. وفي كل خطوة من العملية، يتم إجراء التحقق والاعتماد بواسطة مسؤولين مستقلين لديهم أدوار وصلاحيات مختلفة. ويتم تضمين فصل صارم بين المهام وعناصر تحكم متعددة الطبقات في التصميم لضمان أن تكون القوى العاملة الرقمية ذات موثوقية وقابلة للتوسع وفعّالة وآمنة ومتوافقة.



الشكل 8: نموذج النشر المتقدم لدعم SDLC بشكل كامل

التسجيل والمراقبة

تُعد الإمكانات الشاملة لإعداد التقارير والمراقبة وعمل سجل للتدقيق مكونات ضرورية للبنية الأمنية في أي حل من حلول تكنولوجيا المعلومات البارزة. ومنصة Automation Anywhere Enterprise ليست استثناءً.

فعبر هذه المنصة، يتم تسجيل تفاصيل الأحداث (مَن وماذا ومتى وأين والنتيجة) بشكل تلقائي لأكثر من 60 نوعًا من إجراءات المستخدمين / الكيانات، والتي تشمل عمليات الإنشاء والتعديل والتمكين والتعطيل والإزالة للمستخدمين والروبوتات ومنتجي الروبوتات ومشغّلي الروبوتات. تتحقق خدمة "عدم الإنكار" عبر الجمع بين التسجيل التلقائي، ربط كل نشاط بهوية محددة، وتطبيق سياسة "القراءة فقط" بشكل افتراضي. يمكن أيضًا توظيف RBAC للتحكم بطريقة محكمة في الأدوار التي يمكن لها رؤية سجلات التدقيق من البداية.

ومن منظور المراقبة، يمكن الوصول إلى التقارير ولوحات المعلومات التي تخضع للتشغيل الآلي من داخل غرفة التحكم كما يمكن تخصيصها لتحديد الأنشطة غير الطبيعية وإصدار تنبيه بشأنها (أو أي تفاصيل أخرى مهمة لفريق الأمن أو التشغيل الآلي). وبالإضافة إلى ذلك، تدعم إمكانية تصدير السجلات استخدام البنية التحتية الأخرى للتحليلات وإعداد التقارير والتحقيق في الحوادث والتصدي لها، المستخدمة بالفعل بواسطة المؤسسة، مثل SIEM وUEBA وأدوات التحليلات المتقدمة.

إمكانات إضافية لدعم الأمن والمرونة لدى المؤسسة

تقدم منصة Automation Anywhere Enterprise المزيد من الدعم للأهداف الأمنية والأهداف المتعلقة بالمرونة لدى المؤسسة من خلال:

+ بنية مكونات موزعة (ومرنة) يمكنها أن "تتوافق" بسلاسة مع العمليات والبنية التحتية لقابلية الوصول العالية / مواجهة الكوارث (HA/DR) الموجودة لدى المؤسسة
+ نظام تحكم تكاملي في الإصدار (Apache Subversion) والذي بإمكانه، بالاقتران مع ميزات RBAC واسعة النطاق بالمنصة، تطبيق سياسة وعمليات صارمة للغاية وإنفاذها لإدارة التغييرات
+ أدوات مثل إطاري العمل Hibernate وReactJS أثناء تطوير كود المنصة للمساهمة في منع التأثُّر بالهجمات الشائعة (مثل حقن SQL وهجوم حقن الشفرة المصدريّة عبر موقع وسيط)
+ خطة أمنية / بروتوكول أمني لتطوير التعليمة البرمجية التي تتطلب مسحًا مستمرًا متعدد الأدوات ومتعدد الطبقات لاكتشاف مواطن ضعف البرمجيات وإزالتها

يمكن العثور على المزيد من التفاصيل بشأن هذه الإمكانات وعناصر التحكم ووسائل الحماية والإمكانات الأمنية الأخرى التي تُعد جزءًا من منصة Automation Anywhere Enterprise هنا: "Automation Anywhere Enterprise: Security Architecture" (بنية الأمان).

يحمل التشغيل الآلي للعمليات الروبوتية وعودًا كبيرة للمؤسسات الحديثة التي تتطلّع إلى خفض التكاليف التشغيلية وزيادة رضا العملاء وتحقيق التفوق في المنافسة. وباعتبارها منصة القوى العاملة الرقمية الرائدة في الأسواق، تساهم Automation Anywhere Enterprise في تحقيق أقصى قدر ممكن من هذه المنافع وغيرها من المنافع الأخرى ليس فقط من خلال تحقيق ميزات سهولة الاستخدام وقابلية التوسع والموثوقية المطلوبة لإحراز النجاح، بل أيضًا من خلال تحقيق الأمن على المستوى المؤسسي والذي يُعد مطلوبًا للحفاظ على خصوصية بيئة التشغيل الآلي بكاملها وسلامتها وتوفرها.

للمزيد من المعلومات عن منصة Automation Anywhere Enterprise، الرجاء زيارة:
https://www.automationanywhere.com/products/enterprise.