خصوصية بيانات العميل تأتي في المقام الأول على مستوى الشبكة السحابية لدى Automation Anywhere

تمثل مجموعة الخدمات السحابية التي تحمل علامة Automation Anywhere® منصة تقديم الخدمات المستضافة. وتتضمن مجموعة الخدمات السحابية Control Room (غرفة تحكم) متكاملة وقدرات إنشاء الروبوتات بحيث تتم استضافتها على الشبكة السحابية، جنبًا إلى جنب مع القدرة على تشغيل عُقد Bot Runner المتصلة بالشبكة السحابية على البنية التحتية للعملاء. كما يمكن أيضًا استضافة منتجات إضافية، مثل IQ Bot™، على الشبكة السحابية.

تم تصميم عرض الخدمات السحابية لضمان خصوصية البيانات والذي يعمل وفقًا للائحة العامة لحماية البيانات (GDPR) ومبادئ خصوصية البيانات وإرشاداتها الأخرى.

أمن البيانات

تعتمد بنية النشر نهج "الخصوصية أولاً" لحماية بيانات العملاء والبنية التحتية لديهم.

يتم تشفير اتصال البيانات ما بين Bot Runner على شبكة العملاء وControl Room (غرفة التحكم) الموجودة على الشبكة السحابية. ويتم استخدام بروتوكولات التشفير الآمنة مثل HTTPS ونظام TLS 1.2 لتشفير البيانات المتنقلة. وبالنسبة للبيانات المخزنة على الشبكة السحابية، يتم استخدام تشفير البيانات المخزّنة غير النشطة (على سبيل المثال، معيار التشفير "AES 256-bit").

يتم وصف الوضع الأمني بالكامل، الذي يشمل العمليات السحابية التي يتم نشر العرض السحابي بناءً عليها وتقنيات التشفير وأمن شبكة البيئة، في "دليل عمليات أمن الشبكة السحابية" المتوفر على هذا الرابط <insert URL>

جمع البيانات

يشمل نموذج النشر عملاء يصممون الروبوتات ويديرون عمليات نشر الروبوتات من خلال Control Room (غرفة التحكم) على الشبكة السحابية. وبمجرد تصميم الروبوتات، يتم اختبارها ونشرها للتنفيذ على البنية التحتية الحاسوبية لدى المستخدمين.

يصف الجدول أدناه البيانات التي تم جمعها لمجموعة الخدمات السحابية من Automation Anywhere.
ويقدم الجدول إرشادات بشأن البيانات التي يمكن استخدامها لتحديد هوية شخص طبيعي.

عنصر البيانات	فئة البيانات	الوصف
اسم المستخدم	بيانات شخصية	البريد الإلكتروني، الاسم الأول واسم العائلة، الاسم المفضل، المنطقة الزمنية، آخر تسجيل دخول، كلمة المرور، مجموعة الأسئلة، مجال AD
كلمة مرور المستخدم	بيانات شخصية	
مفتاح أمان كلمة المرور	بيانات شخصية	مفتاح أمان كلمة مرور Credential Vault
الوصول إلى جهاز Bot Runer	بيانات شخصية	بيانات اعتماد الوصول واسم المستخدم للجهاز
تعريفات الدور	بيانات شخصية	المسؤول، والمنشئ، وما إلى ذلك.
الأدوار المعينة للمستخدمين والأجهزة والموارد	بيانات شخصية	أدوار المستخدمين
اسم المجال المؤهل بالكامل (FQDN) / عنوان IP لجهاز الروبوت	بيانات شخصية	يمكن تعقب FQDN أو عنوان IP لجهاز لمستخدم ما
تعريف (مستودع) الروبوتات	بيانات التعريف	البيانات المخزنة كجزء من تعريف الروبوت
بيانات اعتماد تطبيق الروبوت	بيانات شخصية	مستخدم التطبيق، رابط URL، المفتاح العام، اسم التوجيه
جداول روبوت غرفة التحكم	بيانات التعريف	إدارة الروبوتات؛ موعد تشغيل الروبوتات ومكان تشغيلها
تعريف سير عمل إدارة عبء العمل (WLM)	بيانات التعريف	موعد تشغيل الروبوتات ومكان تشغيلها وكيفية تسلسلها
سجلات التدقيق	بيانات شخصية	قد تحتوي على معرفات: سجل رسائل الجهاز، سجل رسائل النشر، سجل رسائل البريد الإلكتروني، سجل تنفيذ المهام: (وقت البدء/الانتهاء، معرف المستخدم، الجدول الزمني، اسم التشغيل الآلي، معرف النشر. اسم الجهاز، اسم الروبوت، اسم المستخدم)، سجل تعديل إدارة المستخدم، سجل رسائل Credential Vault، سجلات تغيير قاعدة البيانات والخادم
سجلات الأخطاء	بيانات شخصية	قد تحتوي على معرفات
التحليلات التشغيلية	بيانات التعريف	حالة الخدمة
بيانات الاستخدام	بيانات التعريف	استخدام الميزات، التراخيص التي تم تمكينها، التي تم تجميعها دون معرفات للبيانات الشخصية/بيانات المستخدم. بالنسبة إلى IQ Bot: مثيلات تعلم المستخدمين، والمجالات، والإحصاءات التشغيلية، وتغييرات التحقق، والمستندات التي تم تحميلها، ونتائج الاستخراج.
بيانات الاستخدام	البيانات الشخصية/ بيانات التعريف	مثيلات تعلم المستخدمين، والمجالات، والإحصاءات التشغيلية، وتغييرات التحقق، والمستندات التي تم تحميلها بواسطة المستخدم، ونتائج الاستخراج.

استخدام البيانات

التشغيل والدعم

تعمل العمليات السحابية على مراقبة أنظمة النشر والأداء التشغيلي من أجل تشغيل الخدمة وتوسيع نطاقها ودعمها وفقًا لاتفاقيات مستوى الخدمة (SLA) <link here>. ولا يمكن لشركة Automation Anywhere بشكل عام أن تطلع على بيانات العملاء المذكورة أعلاه.

وعندما تحتاج خدمات الدعم إلى الوصول من أجل استكشاف المشكلات وحلها، لن يفعل موظفو الدعم ذلك إلا بإذن مناسب من العميل.

من أجل تحسين المنتج، ستعمل Automation Anywhere على:

- تحليل بيانات استخدام الميزات لتحسين المنتج - على سبيل المثال، إضافة نظام القياس عن بُعد لتوفير رؤية تشغيلية داخلية بشأن استخدام الميزات. وسيساعد ذلك Automation Anywhere في تحديد الأولويات بالنسبة للتحسينات وإضافتها في المنتج. وتتضمن الأمثلة ما يلي:
    - مراجعة تكرار استخدام أوامر Excel للمساعدة في تحديد أولويات الأوامر المطلوب إضافتها في الإصدارات المستقبلية
    - تقديم توصيات بشأن أفضل الممارسات التشغيلية
    - توفير خدمات الدعم التي سيتم استخدامها للتحديث والتأمين واستكشاف الأخطاء وإصلاحها
    - تخصيص المنتجات وتقديم التوصيات
    - بالنسبة إلى IQ Bot، سيتم استخدام بيانات العملاء لتحسين جودة مهارات التعلّم للذكاء الاصطناعي (AI)

لمزيد من المعلومات حول سياسة خصوصية البيانات في Automation Anywhere، يرجى الرجوع إلى:
https://www.automationanywhere.com/in/privacy

الاحتفاظ بالبيانات بعد إنهاء الاشتراك

ستحتفظ Automation Anywhere ببيانات العملاء والتكوينات (الروبوتات) وبيانات IQ Bot ومعظم السجلات لمدة 30 يومًا بعد انتهاء اشتراك العميل. وقد يتم الاحتفاظ ببعض السجلات لمدة تصل إلى 180 يومًا بعد انتهاء اشتراك العميل.

ويمكن الاطلاع على التفاصيل الكاملة لملحق معالجة البيانات وسياسة الاحتفاظ بها هنا:
https://www.automationanywhere.com/support/DPA.pdf

حماية البيانات

تمتلك Automation Anywhere مجموعة شاملة من ميزات الأمان التي توفر تلقائيًا حماية للبيانات أو تكون قابلة للتهيئة بحكم تصميمها لتوفير حماية للبيانات. وكما هو الحال مع أي تطبيق مؤسسي، فإن الاستخدام المتسق والسليم للضوابط الأمنية يعتمد على المؤسسة التي تستخدم التطبيق المؤسسي. ويتوقف السماح للمستخدمين على مسؤولي تكنولوجيا المعلومات، الذين ينبغي أن ينفذوا ضوابط لضمان عدم إمكانية الوصول إلا للموظفين المصرح لهم.

يجب على مالك البيانات التأكد من أن الموظفين المصرح لهم الذين لديهم حاجة تتعلق بالأعمال هم فقط من يمكنهم الوصول إلى الخدمة. ويمكن منح مستخدمي الشركات الذين لديهم إمكانية الوصول أذونات دقيقة عن طريق التحكم في الوصول القائم على الدور (RBAC). وتضمن نماذج RBAC وجود ضوابط مزدوجة والفصل بين الواجبات داخل العمليات. كما يمكن تنفيذ الأذونات لجميع جوانب عملية المنتج، بما في ذلك بيانات الاعتماد، والروبوتات، وأدوات Bot Runner، وأدوات Bot Creator، والجداول الزمنية للروبوتات، ومثيلات تعلم IQ Bot، والوصول إلى سجل التدقيق، وقوائم انتظار إدارة عبء العمل، والمجموعات.

توفر Automation Anywhere إمكانات تدقيق كاملة حيث تتم مراجعة جميع إجراءات المستخدم داخل المنصة، مما يوفر سجلات لجميع عمليات الوصول والإجراءات التي يتخذها موظفو العمليات. ويتم تشغيل التدقيق آليًا لجميع الأدوار المتميزة وغير المتميزة وفقًا لأفضل الممارسات كما هو محدد في NIST AC-6.

ونظرًا لأن الروبوتات هي برمجيات مطورة بواسطة خبراء أعمال العملاء، يلزم تنفيذ أفضل العمليات اللازمة لتأمين دورة حياة تطوير البرمجيات (SDLC) من قِبل العملاء تبعًا لذلك. ولتحقيق هذه الغاية، تدعم Automation Anywhere فصل بيئات التطوير والاختبار والإنتاج من خلال مجموعة من عمليات النشر المنفصلة ونماذج RBAC كما هو موضح أعلاه.

تقديم البيانات باسم مستعار

تتطلب لائحة GDPR على وجه التحديد تقديم البيانات باسم مستعار كتدبير تقني مناسب لحماية البيانات. ويعني تقديم البيانات باسم مستعار تحويل البيانات إلى معرفات صورية. وهذا يعطي المراقِب والمعالج طريقة لمعالجة البيانات بحيث لم يعد من الممكن استخدام البيانات للتعرُّف على هوية شخص طبيعي من دون المعلومات الإضافية التي يتم الاحتفاظ بها بشكل منفصل. وعمليات الترميز هي نهج آخر يحوّل البيانات بحيث يمكن الرجوع إليها لاحقًا ولكن من منظور البيانات التي تم ترميزها بحيث لا يمكن استخدامها لتحديد هوية شخص طبيعي.

توصي Automation Anywhere بتنفيذ عملية تقديم البيانات باسم مستعار في بيئات الاختبار والتطوير. وبالنسبة لروبوتات IQ Bot، ستتم معالجة المستندات والصور في بيئة الإنتاج من خلال معلومات المستخدم الحقيقية. ولا توجد إمكانية تقنية لتقديم هذه المستندات باسم مستعار تلقائيًا واستخدام IQ Bot.

الاحتفاظ بالبيانات في Control Room (غرفة التحكم)

هناك حالات حيث يتم الاحتفاظ بالبيانات داخل قواعد البيانات التي تدعم Control Room (غرفة التحكم). وعلى وجه التحديد، عند استخدام إدارة عبء العمل، وIQ Bot و Bot Insight™ (الإصدار المستقبلي). وفي جميع الحالات المتعلقة بالاحتفاظ بالبيانات في Control Room (غرفة التحكم)، تقلل عملية تقديم البيانات باسم مستعار وعملية الترميز من جهود المراقِب والمعالج اللازمة للامتثال للائحة GDPR. وأيضًا، عند تمكين السجلات لمعلومات التصحيح، مثل اسم المستخدم (مستخدمو المنصة)، سيتم الاحتفاظ بها في السجلات.

إدارة عبء العمل وقوائم الانتظار

عند استخدام إدارة عبء العمل (الإصدار المستقبلي) لنشر عدة روبوتات لإجراء التشغيل الآلي ذاته، يتم تخزين عناصر العمل التي يتم وضعها في قوائم الانتظار في قاعدة بيانات Control Room (غرفة التحكم). ومن خلال واجهة مستخدم Control Room (غرفة التحكم)، قد يتم الاستعلام عن أي عنصر عمل ومراجعته وحذفه. وعند معالجة البيانات الشخصية في عناصر العمل، يمكن حذف قوائم الانتظار بشكل دوري.

من الممكن إضافة بيانات اعتماد المستخدم وحذفها من قِبل أي مسؤول لديه الامتيازات المناسبة، التي تم تعيينها بواسطة الدور المناسب. كما تدعم Control Room (غرفة التحكم) الاستعلام عن أي بيانات اعتماد ومراجعتها وحذفها في أي وقت.

توفر Control Room (غرفة التحكم) الوسائل اللازمة لإعداد حسابات المستخدمين وإزالتها باستخدام العناصر المناسبة للتحكم في الوصول القائم على الدور. ويتولّى مسؤول المؤسسة توفير إمكانية الوصول المناسبة للمستخدمين والموارد. ويجب على المسؤول وضع سياسة تحدد مستوى الوصول المطلوب وفقًا للإرشادات المتعلقة بخصوصية بيانات المستخدم والشركة. وإذا طلب مستخدم فردي الوصول إلى معلوماته الشخصية أو فرض قيود عليها، يجب عليه الاتصال بمسؤول العميل. كما يمكن لمسؤولي العميل حذف حسابات المستخدم الموجودة في Control Room (غرفة التحكم).

لمزيد من التفاصيل فيما يخص الاستفسارات المتعلقة بخصوصية البيانات المحددة بواسطة لائحة GDPR ونُسخ البيانات الشخصية، توفر Automation Anywhere الموقع التالي نموذج طلب حقوق الوصول لصاحب البيانات.

الملخص

إن العروض القائمة على الشبكات السحابية والتي تُعد ضرورية للأعمال يجب أن تقدم حلولاً تضمن تأمين الوصول والحفاظ على خصوصية البيانات باعتبارهما من أهم الأولويات في جميع الأحوال.

ومن ثمّ، صُممت مجموعة الخدمات السحابية من Automation Anywhere لتلبية الإرشادات التشغيلية الصعبة بل وتجاوزها، وكان هذا لسبب وجيه: فنحن نضع خصوصية العملاء وأمنهم في المقام الأول عند تقديم حلول التشغيل الآلي إليهم.

لمزيد من المعلومات حول حلول Automation Anywhere السحابية غير المسبوقة، انتقل إلى الشبكة السحابية.