AUTOMATION ANYWHERE

机器人流程自动化的企业级安全性

引言

人们从 20 多年前就开始投资于业务流程自动化技术，为什么至今仍只有不到 20% 的任务实现了自动化？主要原因在于 85% 的企业系统缺少完善定义的 API，结果导致 IT 部门积压的来自业务部门的集成要求越来越多。

机器人流程自动化的形成背景是希望让企业用户能够构建软件机器人，像人类那样与企业系统互动。RPA 机器人可以像人一样使用凭据登录企业应用程序，自动执行涉及任何企业应用程序（包括不含 API 的旧应用程序）的任务。自动化技术的潜在应用涵盖广泛的业务领域，办理理赔、办理贷款、核对账目、创建/提交发票以及生成报告只是其中的少数几个例子。

不难看到，使用 RPA 能带来诸多效益，如大幅减少时间和成本、提高客户满意度、提升员工士气，以及形成竞争对手所不具备的领先优势。但要充分实现这些效益，必须具备一个覆盖整个企业的解决方案。

实现自动化的其中一些重要条件包括提供强大的可靠性、可扩展性和广泛的功能组合，让适用性和使用性最大化。但这些要素并未涵盖企业最重要的要求：端到端安全性。一个成熟稳健的安全架构，搭载全面支持核心原则所需的各种功能，比如最低权限和职责分工，同时为重要应用及相关的敏感数据提供端到端保护，这些都是关键任务。

本白皮书概述市场领先的数字化劳动力平台 Automation Anywhere Enterprise 所体现出来的业内最高标准的企业级安全性。

“

不难看到，使用 RPA 能带来诸多效益，如大幅减少时间和成本、提高客户满意度、提升员工士气，以及形成竞争对手所不具备的领先优势。但要充分实现这些效益，必须具备一个覆盖整个企业的解决方案。

架构和运行

要了解在全企业实现 RPA 所需具备的安全控制特性，就必须了解组成解决方案的组件及其运行。

核心组件

从图 **1** 可以看到，Automation Anywhere Enterprise 的核心模块是控制室、机器人创造程序和机器人运行程序。

控制室

控制室是自动化环境的大脑。它是一个基于 Windows 服务器的管理系统，内置集成数据库，提供一个集中统一的总体系统管理视图。RPA 操作员也通过控制室协调数字化劳动力，即调度、部署、执行、监控和管理公司机器人的运行。此外，内置的版本控制功能（Apache Subversion 服务器）能促进多用户协作，加强变更管理优秀实践，建立一个可随时用于实际部署的现成机器人的中央存储库。

机器人创造程序

机器人创造程序用于构建机器人。机器人创造程序是一个在工作站或虚拟机上运行的 Windows 桌面应用，供业务流程专家创建机器人和测试其自动化性能。专家使用机器人编辑器创建机器人，再使用本地的非实际部署测试数据和应用实例，在机器人运行程序的帮助下测试机器人。成功完成测试后（例如，测试性能、数据完整性和安全性），将机器人检入控制室存储库，用于实际部署。

机器人运行程序

机器人运行程序将机器人投入到工作中。机器人运行程序和机器人创造程序一样使用相同的应用程序代码，但许可证密钥不同。它在实际部署环境中执行机器人，即使用目标应用程序的实际部署实例和实际部署数据存储库。事实上，机器人运行程序只能运行机器人，因为它们不具备创建和编辑功能。为了实现更加可靠的大规模运行，它还支持机器人运行程序集中池。

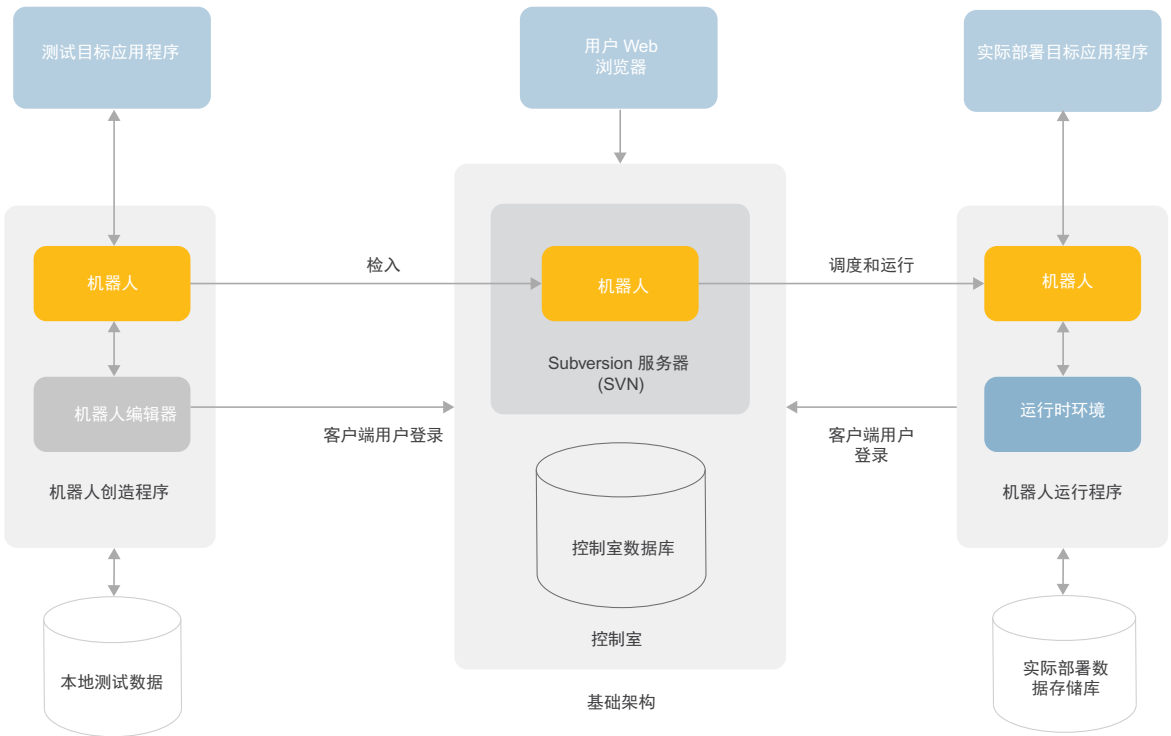

图 1： Automation Anywhere Enterprise 基础架构

其他企业级组件

要实现大规模运行，还必须考虑另外两个与要实现企业级部署的组织相关的重要 RPA 解决方案：按需扩展和 Bot Insight。

按需扩展

Automation Anywhere Enterprise 利用 Amazon Web Services (AWS) 公有云，高效提供 RPA 即服务及所有参与者功能，包括灵活扩充/缩减、按使用量计费、无限制横向扩展以及持续监控机器人运行程序基础设施并记录审核日志。因此能实现多节点高可用性，保障以 SLA 为驱动的性能和业务连续性，即使是在自动化工作量剧烈波动时期也不受影响。

Bot Insight

Bot Insight 作为一个完全集成在控制室中的子系统，能够近乎实时地分析机器人运行状况和业务流程数据。Bot Insight 使用先进算法，自动生成每个机器人独特的可定制控制面板。Bot Insight 提供精细的机器人运行事件日志，支持灵敏警报、点对点发现、互动钻取、时间序列分析以及运行/业务流程全面分析。此外，还可以将所有数据导出为安全信息和事件管理 (SIEM) 日志，用于进一步分析、调查和报告。

工作中的机器人：两种类型的自动化

在探索 Automation Anywhere Enterprise 的高安全性功能之前，还有最后一个需要澄清的事实是，自动化分为两种基本类型：有人监督的自动化和无人监督的自动化。

有人监督的自动化是指用户登录机器人运行程序计算机，观察和/或主动支持机器人执行操作。需要用户在场可能是因为机器人服务于在工作中提供协助的实用型功能，也可能是因为机器人执行批量作业，要求用户定期输入或根据情况做出指示。有人监督的自动化也称为前端自动化。

无人监督的自动化正如其名，在执行操作时无需企业用户或操作员干预。对无人监督的自动化进行管理的操作员通常对机器人、实现自动化的应用程序或自动化的目的不甚了解。操作员与业务单位共同调度机器人在机器人运行程序上运行。在执行过程中，操作员对工作中的机器人的运行状况进行监控，例如 CPU、内存和存储使用情况，确保在执行过程中不出现任何错误或异常。控制室控制面板显示机器人在工作过程中的所有详细运行状况。如果无人监督的自动化因为遇到错误而无法完成任务，操作员可能要按照程序修复并重启自动化，或者将问题上报至 RPA 团队或业务单位进行诊断和修复。

多重企业 RPA 安全性
多重身份识别和验证

Automation Anywhere Enterprise 安全基础架构的一个核心原则是在进行任何访问或操作前，必须先对相关实体进行身份验证。这条原则对人和机器人同等适用。因此，有人监督的自动化和无人监督的自动化都实施多重身份验证流程。

谁是谁：标准企业身份验证

可以使用多重凭据和人物角色。我们来看一个简单的企业身份验证情景（请参见**图 2**）。企业用户 Alice 完成身份验证后，进入 Windows 工作站。随后，Alice 登录远程运行的应用程序，通过 Windows Domain Active Directory 登录凭据或 Kerberos 进行身份验证，这取决于拥有有效票证的工作站。在此情景中，身份验证链涉及一位用户及其凭据。

图 2： 标准企业身份验证

现在来看看有人监督的自动化情景，如**图 3** 所示。在此案例中，用户 Bob 正在测试机器人或运行有人监督的自动化，这是他的日常工作内容。在第 1 步，他使用个人凭据完成身份验证后，进入机器人运行程序工作站（和上一个情景中的 Alice 一样）。在第 2 步，他启动 Automation Anywhere Enterprise 客户端，使用用户名和密码进入控制室，因此让客户端软件得以通过身份验证，进入控制室。在第 3 步，他运行机器人，而机器人需要在完成身份验证后访问应用程序。在这个步骤中，机器人使用的凭据可以存储在 Enterprise 凭据保管库中，由机器人在运行时提取凭据，或者传递 Bob 的个人凭据（根据他的工作站和相同领域的应用程序服务器提供的许可）。无论采用哪一种方法，都总共实施了三重身份识别和验证。

无人监督的情景（如**图 4** 所示）也使用三重身份验证，但存在一些差异。在此案例中，用户 Charles 先完成身份验证，进入控制室，然后选择一个机器人立即运行或在预定的时间运行。

在第 2 步，机器人启动执行的时间一到，控制室就开始使用 BotRunnerUser 凭据自动登录到机器人运行程序工作站。机器人下载到本地播放器功能（第 3 步）并启动执行后，便使用 BotApplicationUser 凭据进行身份验证，进入目标应用程序（第 4 步）。同有人监督的自动化情景一样，可以使用从凭据保管库提取的 BotApplicationUser 凭据，也可以使用传递的 BotRunnerUser 凭据。

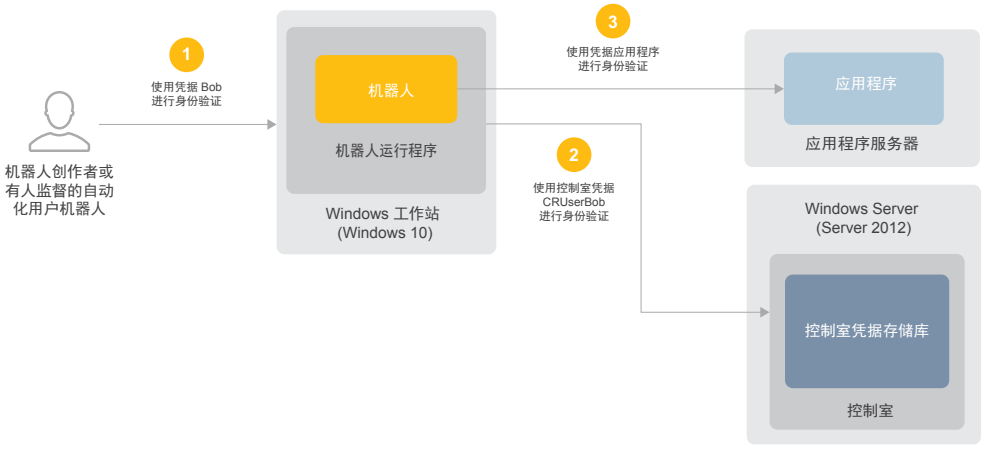

图 3： 有人监督的自动化情景的身份验证流程

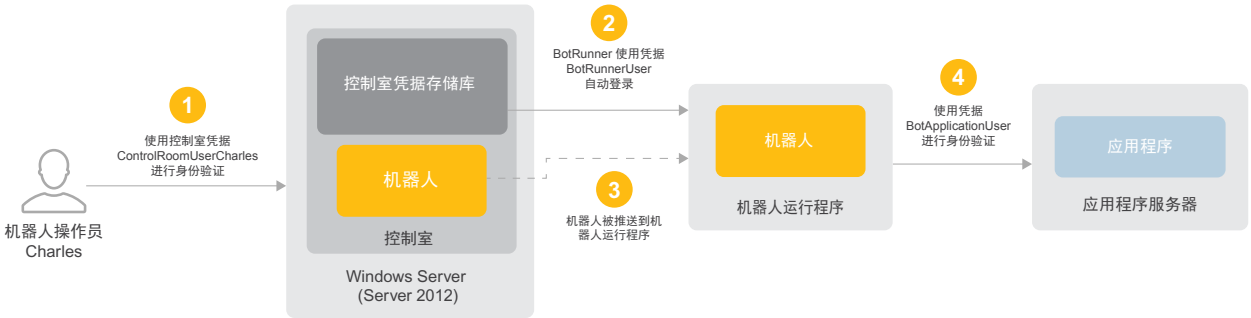

图 4： 无人监督的自动化情景的身份验证流程

身份验证选项和 IAM 集成

支持的控制室身份验证选项包括使用 LDAP 的活动目录、使用 Kerberos 的活动目录，以及使用嵌入式凭据保管库的本地身份验证（将在后面进行讨论）。

其他可用于企业部署的身份和访问权限管理选项包括：

+ 支持基于 SAML 2.0 的单点登录
+ 集成第三方访问权限/凭据管理解决方案（例如，CyberArk、One Identity 和 Thycotic）

全面的基于角色的访问控制

顺利完成身份验证只是执行了 Automation Anywhere Enterprise 安全基础架构提供的第一层强制访问控制。支持精细的基于角色的访问控制 (RBAC) 同样重要，尤其是从遵循最低权限和职责分工这两个核心原则来说。

在 RPA 平台的基础架构和主要功能中，要考虑五个截然不同的角色（请参见**图 1**）。机器人构建者使用机器人创造程序收集业务逻辑，并创建相应的自动化。机器人构建者使用测试应用程序和数据集，使实际部署系统在开发阶段不受影响。单个机器人通常会经历多个不同的迭代和版本，这不仅发生在初步开发期间，也发生在每一次更新相关业务流程和/或目标应用程序时。机器人测试者也使用机器人创造程序测试机器人性能、数据完整性和安全性，确保每个机器人以安全的方式按预期工作。机器人测试者是机器人获得授权所需经历的第二个阶段。在此阶段后，机器人才能使用实际部署数据和应用程序开始运行。

机器人经过测试和安全审核后，机器人促进者与机器人构建者/机器人测试者共同指定要在实际部署中使用的机器人版本。这是机器人操作者能够看到的唯一版本。机器人操作者与业务单位配合，调度和运行机器人。机器人操作者还负责在控制室中监控机器人性能，包括排查可能出现的任何运行时问题。最后，由 RPA 管理员负责平台的总体管理，包括配置组件、界面以及所有角色/权限。

先进的职责分工

这套核心角色代表了 RBAC 的一个基准点，但在 Automation Anywhere Enterprise 平台中，还可以实现更高程度的职责分工。管理员使用嵌入式角色创建向导，可以轻松定义自定义角色，为所有控制室对象和功能设置特权/权限，包括用户管理、授权许可、凭据保管库、机器人运行程序集、机器人调度、机器人运行/控制面板和审核日志。选择每一个权限后，向导会动态地添加临时/衍生权限步骤。

例如，选中 BOTS › View my bots › Run My bots 权限后（请参见**图 5**），工作流将添加一个步骤，指示授予访问权限的具体机器人文件夹（即，机器人集）。最终能够充分建立高度精确的角色和精细的访问权限控制，满足最严格的、安全的法规监管环境的要求。

角色	描述
RPA 操作者	管理系统（配置组件、角色、界面）
机器人构建者	使用任务编辑器创建机器人并执行基本功能测试的业务流程专家
机器人测试者	审查机器人功能准确性、性能和安全的质控测试人员
机器人促进者	批准并将机器人在开发、测试和实际部署阶段之间移动的管理员
RPA 操作者	调度、运行和监控机器人性能的操作员

表 1： Automation Anywhere Enterprise 中的主要 RPA 角色

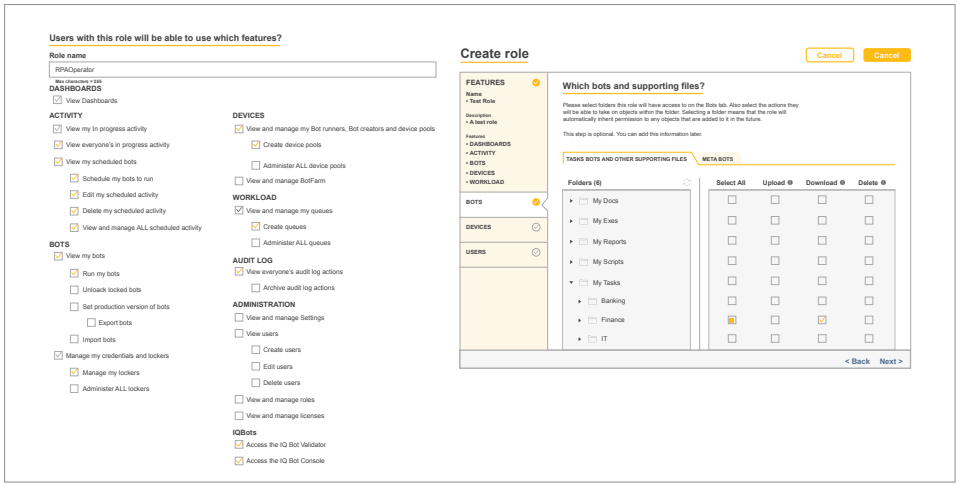

图 5：使用精细授权创建角色

独立控制平面

除了拥有广泛的 RBAC 能力外，Automation Anywhere Enterprise 还具备一项内在能力，能够通过一个基础架构完全分离机器人开发任务和机器人执行任务，实现合理的职责分工。

机器人创造程序只能将机器人上传到控制室的版本控制系统中，以及从该系统下载机器人。同时，机器人运行程序只能执行机器人。它们没有权限创建机器人和执行功能测试。通过基础架构执行职责分工的模式构成双重授权，符合美国国家标准与技术研究所 (National Institute of Standards and Technologies, NIST) 的优秀实践，因为它需要开发者和企业用户最终能够实现业务流程自动化，这是它的最低要求。

独立处理领域

体现平台 RBAC 能力的一个有力用例是建立独立的处理领域（请参见**图 6**），这对于大型企业来说尤其有用。要实现这一目的，可以针对每一个目标领域严格整理机器人，并将机器人存储到控制室的相应文件夹中。

例如：与财务应用程序相关的机器人应放在财务文件夹中，与人力资源相关的机器人则应放在人力资源文件夹中。然后再向财务部门的机器人操作者分配仅适用于财务机器人和财务机器人运行程序的权限；人力资源部门的机器人操作者将获得仅适用于人力资源机器人和人力资源机器人运行程序的权限。对于其他处理/自动化领域，也是一样的道理（请参见**图 6**）。

这样进一步在 OU/领域层面实现了职责分工以及相关应用和数据分离，因为操作者个人无法查看或操作超出其特定领域的机器人。

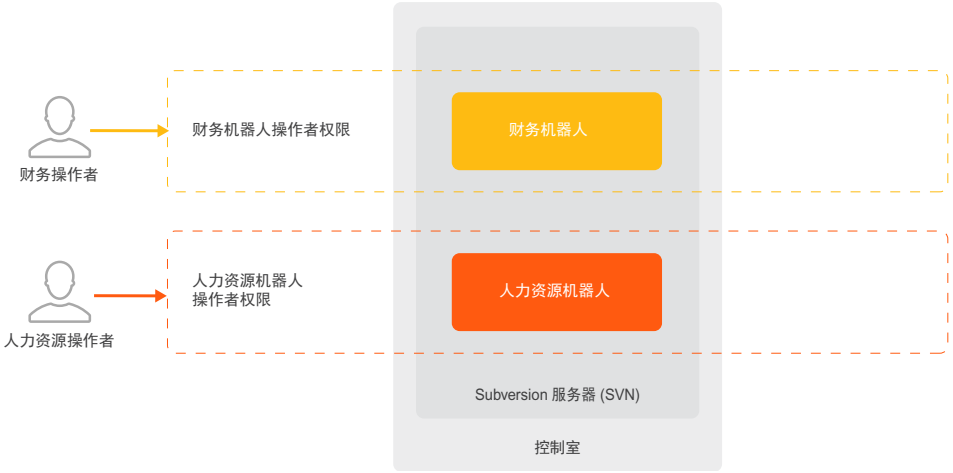

图 6：支持独立处理领域

端到端数据保护

多重身份验证和精细的访问控制是创造一个严格控制的环境的关键。端到端数据保护也是一样。它对于维护关键业务流程、敏感数据及相关秘密（例如凭据）的机密性和完整性也十分必要。

Automation Anywhere Enterprise 平台的嵌入式凭据保管库解决了这一需求，提供各种保障措施，不仅保护静态数据和传输中的数据，也保护在个别系统上使用的数据。

加密密钥和凭据保管库

图 7 显示平台使用的主要加密密钥及其与凭据保管库的关系。所有加密均通过 FIPS 140-2 1 级验证密码模块完成。

在安装期间（**图 7** 的左侧部分），系统生成 RSA 2048 位公钥/私钥对和 AES 256 位密钥。RSA 2048 密钥对的私钥被称为主密钥，AES 256 密钥被称为数据密钥。执行安装的管理员可以看到主密钥，将其安全保存在系统之外的物理场所。公钥用于对数据密钥加密。随后，公钥和加密的数据密钥均存储在数据库。使用时，通过 Microsoft 数据保护 API (DPAPI) 将所有密钥和加密的数据放在加密的安全内存中。

在控制室启动或重启过程中（**图 7** 的右侧部分），系统提示管理员提供主密钥。使用主密钥从数据库提取加密的数据密钥并解密。现在可以随时使用数据密钥。系统将数据存储到凭据保管库，并从保管库提取数据，而数据密钥则用于对该数据进行加密和解密。

凭据保管库用于存储由系统管理的所有凭据和关键系统配置数据。它还可用于存储在组织的自动化中使用的任何其他敏感数据（例如，名称-值对）。这样一来，机器人构建者可以避免在自动化中直接对凭据和其他敏感数据/参数进行硬编码的不安全实践。

保护静态数据

除了对本地凭据加密以及选择机器人要使用的运行时数据外，凭据保管库还能够安全存储敏感的配置参数以及与集成的版本控制和电子邮件服务相关的详细信息。

保护传输中的数据

客户端的所有网络服务和控制室均通过安全传输层协议 (TLS) 1.2 保障在不同组件间传输的数据的安全性和完整性。

机器人创造程序/运行程序进行身份验证所使用的凭据会先进行加密，然后再通过 TLS 安全连接进行提交。额外加密层不仅能预防网络栈问题（例如 Heartbleed），而且当前端负载均衡器终止外层 TLS 连接时能防止凭据泄露。

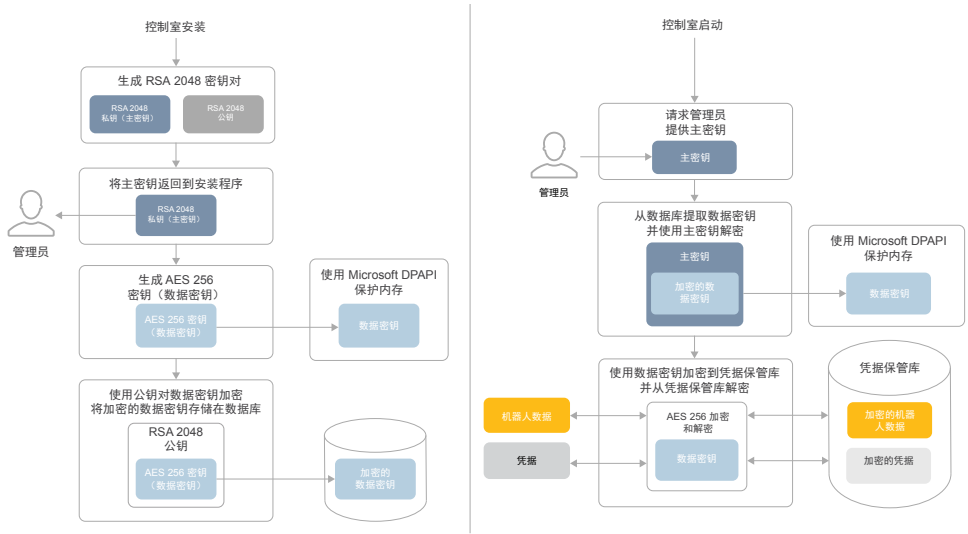

图 7： Automation Anywhere Enterprise 加密基础架构

保护使用中的数据

运行时安全从分布式凭据保护开始。具体来说，机器人运行程序中不存储任何本地凭据。从凭据保管库中动态提取并在自动化中使用的凭据和其他数据仅以加密形式保留在易失性存储器中，一旦相关机器人完成执行过程，便立即擦除。

为了防止在运行时期间未经授权访问机密信息（即数据泄露）或篡改机器人，还提供了其他功能和配置选项，包括：

+ 隐身模式 - 本地屏幕上不显示程序窗口，且登录的用户可以选择禁用机器人创造程序和机器人运行程序截图，防止屏幕上显示的敏感信息存储在机器人中
+ 输入锁定 - 能够禁用正在运行自动化的计算机上的鼠标和键盘
+ 时间限制 - 能够设定时间限制，如果自动化在超过时间限制后仍未完成执行过程，将终止自动化。
+ 集中控制 - 能够通过控制室集中控制正在远程运行的自动化的运行（即，暂停运行、恢复运行、停止运行）

安全软件开发生命周期 (SDLC) 支持

为了在自动化环境中提供最高水平的控制和保障，前面描述的基本部署情景可“扩展”到更多安全软件开发生命周期 (SDLC) 优秀实践，例如 FISMA、FedRamp 和 PCI DSS 所要求的优秀实践。如此一来，先进的部署模式提供三个截然不同的 RPA 区域，分别用于开发、用户验收测试 (UAT) 和实际部署（请参见图 8）。每个区域都通过具有指定的独特角色和权限的不同用户组实现逻辑分离（隔离）。竖直虚线表示网络分割和防火墙。

在基本部署模式中，机器人生命周期的最初阶段是开发。一旦机器人构建者对机器人感到满意，UAT 机器人促进者会将机器人从开发版本控制存储库 (SVN) 转移到 UAT 存储库。UAT 区域的唯一目的是测试机器人的准确性、性能和安全性。一旦机器人通过验收测试，实际部署机器人促进者会将机器人转移到实际部署区域。此时，它进入实际部署状态，RPA 操作者可将其用于实际部署应用程序。在流程的每一个阶段，都有具有不同角色和权限的不同管理员执行校验和认证。机器人在设计上内在地实现了严格的职责分工和多重控制，确保数字化劳动力可靠、可扩展、高效、安全、合规。

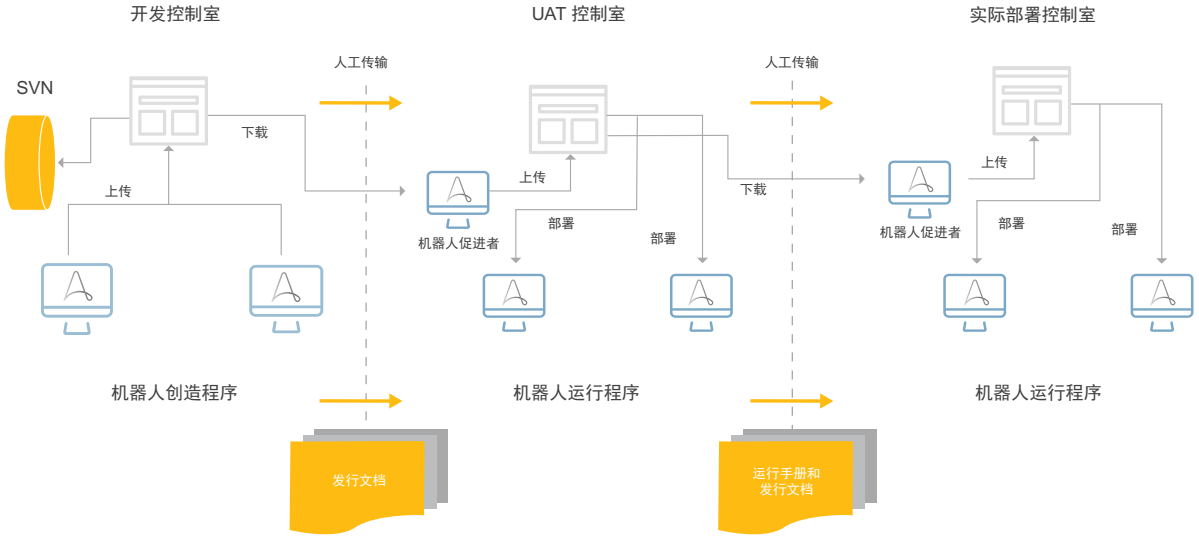

图 8： 提供全面 SDLC 支持的先进部署模式

日志记录和监控

对于任何备受瞩目的 IT 解决方案来说，全面的审核日志记录、监控和报告功能是安全架构的必要组件。Automation Anywhere Enterprise 也不例外。

在整个平台内，能自动收集 60 多种用户/实体操作类型（包括创建、修改、启用、禁用和删除用户、机器人、机器人创造程序和机器人运行程序）的每一个详细信息（操作者、操作内容、操作时间、操作位置和操作结果）。通过结合使用自动收集、将每个活动与特定身份绑定以及默认的只读策略，满足了不可抵赖性要求。还可以利用 RBAC 严格控制能够最先查看审核日志的角色。

从监控性能来说，可在控制室内查看自动化控制面板和报告并进行自定义，以识别异常活动（或者自动化或安全团队认为值得关切的任何其他详细信息）并发出警报。此外还具备导出日志功能，从而能够使用其他分析、报告以及组织正在使用的事件调查/响应基础设施，例如 SIEM、UEBA 和先进分析工具。

更多企业安全性和弹性能力

Automation Anywhere Enterprise 的以下特性能够实现更多企业安全性和弹性目标：

+ 分布式（灵活的）组件架构能够无缝“适配”组织现有高可用性/灾难恢复 (HA/DR) 架构和流程
+ 集成式版本控制系统 (Apache Subversion) 配合平台丰富的 RBAC 功能，能够实现和执行高度可靠的变更管理策略和流程
+ 在开发平台代码期间使用 Hibernate 和 ReactJS 框架等工具，有助于消除易遭受常见攻击的漏洞（例如 SQL 注入和跨站脚本）
+ 用于代码开发的安全计划/协议，需要持续使用多个工具进行多重扫描，检测和消除软件漏洞

有关这些特性以及 Automation Anywhere Enterprise 许多其他控制、保障和安全功能的更多详细信息位于：Automation Anywhere Enterprise：安全架构。

对于那些希望降低运营成本、改善客户体验、获得竞争优势的现代企业来说，机器人流程自动化是一个前景无限的出路。作为市场领先的智能数字化劳动力平台，Automation Anywhere Enterprise 有助于最大程度地创造这些效益，此外还能带来其他更多优势，不仅能提供企业成功运营所需具备的可靠性、可扩展性和使用性特性，还能实现必需的企业级安全性，保护整个自动化环境的机密性、完整性和可用性。

有关 Automation Anywhere Enterprise 的更多信息，请访问：
https://www.automationanywhere.com/products/enterprise.