AUTOMATION ANYWHERE

Segurança de nível empresarial - RPA para ambientes corporativos

INTRODUÇÃO

Por que, após mais de 20 anos de investimento em tecnologias de automação de processos, menos de 20% das tarefas foram automatizadas? O motivo principal é a falta de APIs bem-definidas em 85% dos sistemas corporativos. O resultado é um atraso de TI crescente nas solicitações de integração das áreas de negócios.

A Automação Robótica de Processos nasceu com a visão de empoderamento de usuários empresariais para criar bots de software que podem interagir com sistemas empresariais assim como humanos. Bots e RPA podem entrar em aplicativos empresariais usando credenciais, como humanos, e automatizar tarefas que envolvem qualquer aplicativo empresarial, incluindo aplicativos herdados sem APIs. Processamento de reivindicações, processamento de empréstimos, reconciliações contábeis, criação/envio de faturas e criação de relatório são apenas alguns dos exemplos de possíveis automações que se estendem às diferentes disciplinas empresariais.

É fácil ver o potencial de economia de tempo e dinheiro significativa, satisfação de cliente aprimorada, maior confiança à força de trabalho e a habilidade de criar uma vantagem de comando sobre competidores usando a RPA. No entanto, entender por completo esses ganhos depende de uma solução Enterprise.

Fornecer um conjunto de recursos de confiabilidade e escalabilidade extensivos e sólidos para maximizar aplicabilidade e usabilidade são alguns dos critérios essenciais para automação. Mas esses elementos não cobrem o requisito empresarial mais crítico: segurança de ponta a ponta. Uma arquitetura de segurança robusta com recursos que possibilitam suporte completo para princípios essenciais, como privilégios inferiores e separação de tarefas, enquanto entrega proteção de ponta a ponta para os aplicativos críticos e dados sensíveis, é uma missão difícil.

Esse papel fornece uma visão geral do mais alto padrão da indústria para segurança de nível empresarial, como demonstrado pela plataforma de força de trabalho líder do mercado, Automation Anywhere Enterprise.

“

É fácil ver o potencial de economia de tempo e dinheiro significativa, satisfação de cliente aprimorada, maior confiança à força de trabalho e a habilidade de criar uma vantagem de comando sobre competidores usando a RPA. No entanto, entender por completo esses ganhos depende de uma solução de classe empresarial.

ARQUITETURA E OPERAÇÕES

Entender os controles de segurança necessários para uma implementação da RPA de nível empresarial depende da compreensão dos componentes que incluem a solução e suas operações.

Componentes principais

Como exibido na **Figura 1**, os blocos de construção principais do Automation Anywhere Enterprise são Control Room, os Bot Creators e os Bot Runners.

Control Room

O Control Room funciona como o cérebro do ambiente de automação. É um sistema de gerenciamento baseado no servidor Windows, com um banco de dados integral, que fornece uma exibição unificada para a administração geral do sistema. O Control Room também é onde operadores da RPA vão para orquestrar a força de trabalho digital. Em outras palavras, para agendar, implantar, executar, monitorar e gerenciar a operação dos bots da organização. Além disso, recursos de controle de versão integrados (Apache Subversion Server) facilitam a colaboração multiusuário enquanto impõem as melhores práticas de gerenciamento de mudança e estabelecem um repositório centralizado de bots prontos para produção.

Bot Creator

O Bot Creator é usado para criar bots. Este é um aplicativo da área de trabalho do Windows sendo executado em uma estação de trabalho ou máquina virtual. O Bot Creator é usado por especialistas de processo empresarial que criam e testam suas automações. Os bots são criados utilizando o Editor de bot, enquanto o teste dos bots (usando dados de teste não advindos de produção locais e instâncias de aplicativo) é facilitado pelo Bot Runner. Depois do teste bem-sucedido (por exemplo, para desempenho, integridade de dados e segurança), bots são verificados no repositório do Control Room e tornam-se disponíveis para implantação de produção.

Bot Runner

O Bot Runner coloca os bots para trabalhar. Usando o mesmo código de aplicativo que o Bot Creator, mas com uma chave de licença diferente, o Bot Runner executa bots no ambiente de produção. Isto é, utilizando instâncias de produção do aplicativo alvo e armazenamento de dados de produção. Na verdade, executar bots é tudo o que Bot Runners podem fazer, já que as funções de criação e edição não estão disponíveis para eles. Para operações em grande escala altamente confiáveis, a centralização dos Bot Runners também é suportada.

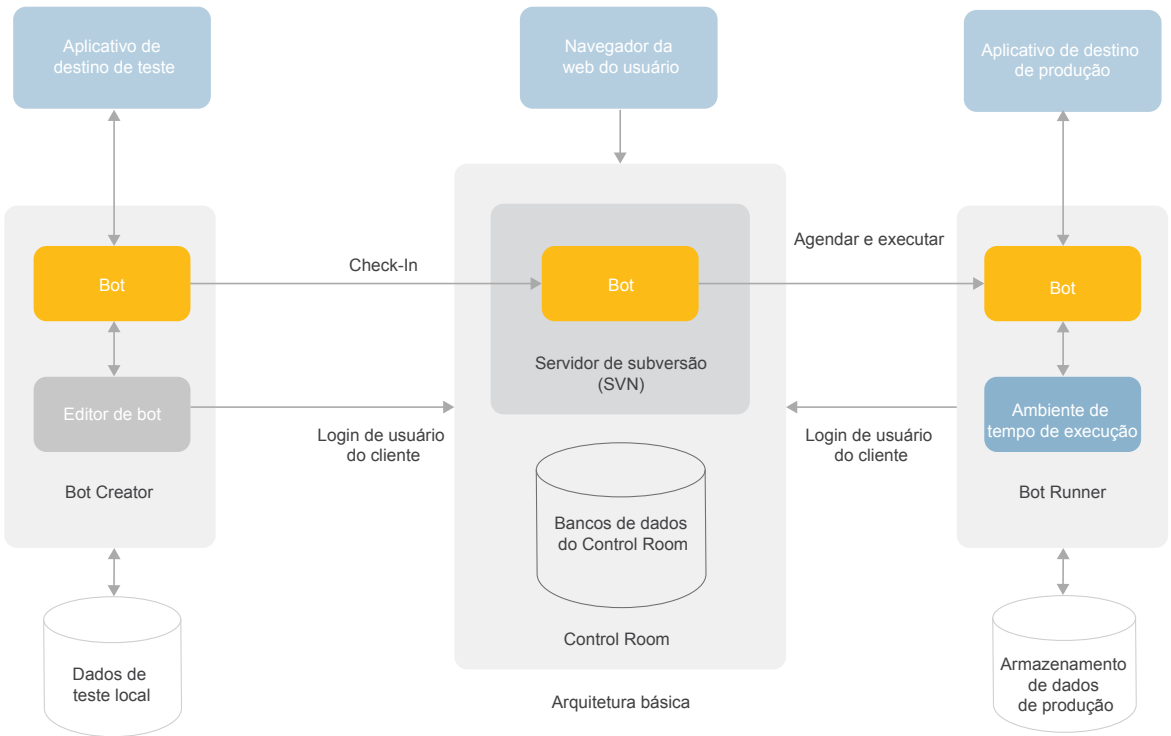

Figura 1: Arquitetura básica do Automation Anywhere Enterprise

Módulos adicionais de nível corporativo

Ao considerar operações de grande escala, dois outros módulos RPA importantes e relevantes a organizações que buscam utilizar implantações de nível empresarial surgem: escalabilidade sob demanda e Bot Insight.

Escalabilidade sob demanda

Com ajuda da utilização de nuvem pública da Amazon Web Services (AWS), o Automation Anywhere Enterprise entrega, de forma eficaz, a RPA como um serviço com todos os recursos de assistente, incluindo aumento/diminuição elástico, medição com base em uso, escalabilidade horizontal ilimitada, monitoramento contínuo e log de auditoria da infraestrutura de Bot Runner. O resultado é alta disponibilidade de nós múltiplos que aprimora o desempenho com base em SLA e continuidade empresarial, mesmo quando há variações drásticas na carga de trabalho de automação.

Bot Insight

Um subsistema completamente integrado dentro do Control Room, o Bot Insight realiza análise quase que em tempo real de operações de bot e dados de processo. O Bot Insight gera automaticamente dashboards personalizáveis usando algoritmos avançados únicos para cada bot. O nível de detalhes que o Bot Insight fornece baseado em logs de evento detalhados sobre operações de bot permite alertas diferenciados, descoberta de ad-hoc, pesquisas interativas, análise de série de tempo e informações abrangentes sobre os processos. Além disso, todos os dados podem ser exportados para logs de informações de segurança e gerenciamento de evento (SIEM) para análise, investigação e relatórios adicionais.

Bots em ação: dois tipos de automações

Um último ponto a ser esclarecido antes de entrar nas funcionalidades de segurança de alto nível do Automation Anywhere Enterprise são os dois tipos básicos de automações: assistido e não assistido.

Uma automação assistida ocorre quando um usuário está logado em uma máquina de Bot Runner para observar e/ou dar suporte ativo à execução do bot. Um dos motivos para haver um usuário presente é que que o bot pode ter uma função de utilitário que ajuda em seu trabalho, ou que o bot realiza trabalho em lote que requer entrada periódica ou direcionamento situacional de um usuário. Automações assistidas também são conhecidas como automações de front office.

Automações não assistidas, como o nome sugere, operam sem a necessidade de um usuário empresarial ou interação de operador. Automações não assistidas geralmente são executadas por um operador que tem pouco conhecimento sobre o bot, o aplicativo sendo automatizado ou o motivo da automação. O operador, no Control Room, agenda bots para executar nos Bot Runners. Durante execução, o operador monitora aspectos operacionais dos bots em execução, como CPU, memória e uso de armazenamento para garantir que eles sejam executados sem quaisquer erros ou exceções. Dashboards do Control Room exibem todos os detalhes operacionais dos bots conforme eles são executados. Se uma automação não assistida não for concluída por conta de um erro, o operador pode implementar procedimentos para corrigir a automação e reiniciá-la; caso contrário, eles serão direcionados para a equipe de RPA ou unidade empresarial para diagnosticar e corrigir o problema.

IDENTIFICAÇÃO E AUTENTICAÇÃO DE MULTICAMADAS DE SEGURANÇA DO RPA

Um princípio fundamental da arquitetura de segurança do Automation Anywhere Enterprise é que nenhum acesso ou ação é permitido sem autenticação prévia da entidade envolvida. Isso aplica-se a humanos e a bots também. O resultado é um processo de autenticação multicamada para automações assistidas e não assistidas.

QUEM É QUEM: AUTENTICAÇÕES TÍPICAS EMPRESARIAIS

Credenciais e identidades podem ser multicamadas. Considere um cenário de autenticação empresarial simples (consulte **Figura 2**). Uma usuária, Alice, se loga no Windows. Alice entra em um aplicativo que está em execução remotamente, autenticando por meio de um login do Active Directory de domínio do Windows ou talvez por Kerberos, baseado em sua estação de trabalho que tem um ticket válido. Neste cenário, a cadeia de autenticação envolve uma única pessoa e suas credenciais.

Figura 2: Autenticação típica empresarial

Agora considere o cenário de automação assistida exibido na **Figura 3**. Neste caso, o usuário Bob está testando um bot ou executando uma automação assistida como parte de um dia típico de trabalho. Na etapa 1, ele loga o Bot Runner usando suas credenciais pessoais (como no cenário de Alice acima). Na etapa 2, ele inicia o cliente Automation Anywhere Enterprise e insere seu ID de usuário do Control Room e senha, autenticando o software de cliente para o Control Room. Na etapa 3, ele executa o bot que, por sua vez, acessa um aplicativo que precisa de autenticação. As credenciais usadas pelo bot nesta etapa podem ser armazenadas no Cofre de credencial empresarial e recuperadas pelo bot durante o tempo de execução, ou podem ser transferências de credencial pessoal do Bob (com base em compensação oferecida pela sua estação de trabalho e o servidor de aplicativo estando no mesmo domínio). De qualquer forma, o resultado são três camadas de identificação e autenticação no total.

Há três camadas de autenticação usadas para o cenário não assistido mostrado na **Figura 4**, embora com um pouco de reviravoltas. Neste caso o usuário, Charles, começa autenticando o Control Room para que ele possa selecionar um bot para a ser executado imediatamente ou em um período agendado.

Na etapa 2, quando o período de execução do bot iniciar, o Control Room inicia um login automático para a estação de trabalho do Bot Runner, usando a credencial do usuário Bot Runner. Depois de um bot ser baixado para a função de reprodução local (Etapa 3) e iniciar sua execução, ele autentica o aplicativo de destino usando a credencial de usuário do aplicativo de bot (Etapa 4). Assim como com o cenário de automação assistida, a credencial de usuário do aplicativo de bot pode ser aquela recuperada do Cofre de credenciais, ou pode ser uma transferência da credencial de usuário do Bot Runner.

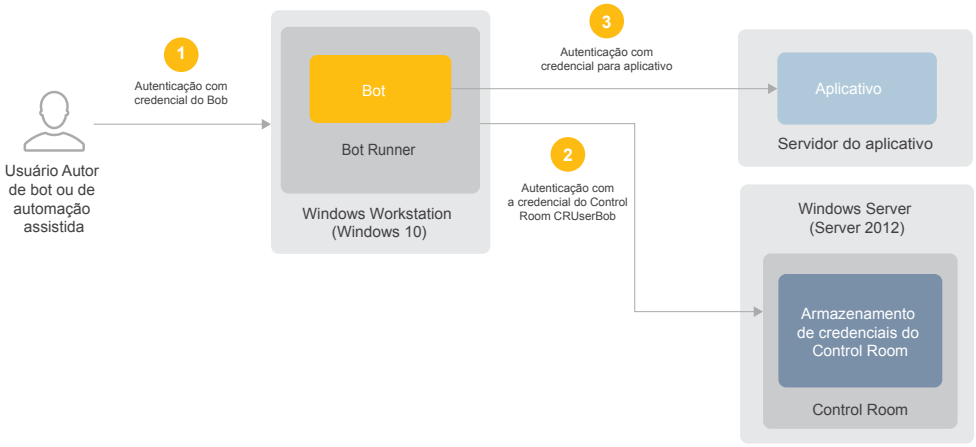

Figura 3: Processo de Autenticação durante automação assistida

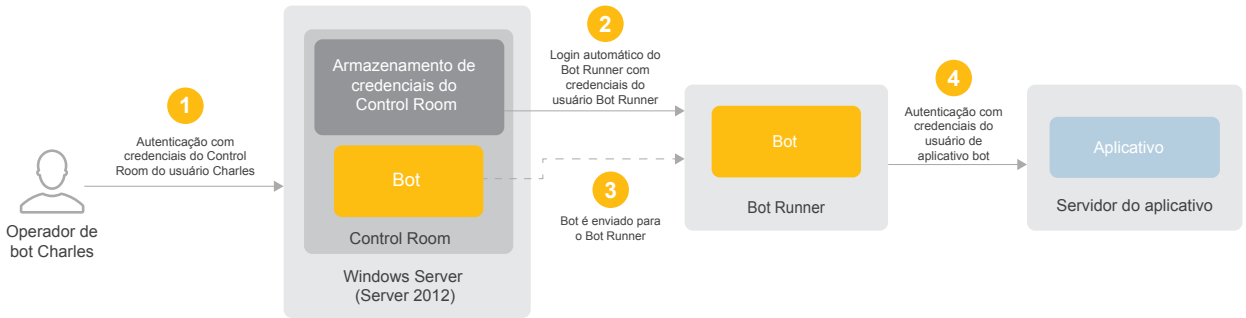

Figura 4: Processo de Autenticação durante automação não assistida

Opções de autenticação e integrações do IAM (Identity and Access Management)

Opções suportadas para autenticação do Control Room incluem Active Directory usando LDAP, Active Directory usando Kerberos e autenticação local usando o Cofre de credenciais integrado (discutido posteriormente neste artigo).

Outras opções de identidade e gerenciamento de acesso disponíveis para implantações empresariais incluem:

+ Suporte ao SAML 2.0 baseado em logon único
+ Integração com soluções de gerenciamento de acesso/credencial privilegiado de terceiros (por exemplo, CyberArk, One Identity e Thycotic)

AMPLO CONTROLE DE ACESSO BASEADO NA FUNÇÃO (RBAC)

A autenticação bem-sucedida é apenas o primeiro nível de execução de controle de acesso obrigatório oferecido pela arquitetura de segurança do Automation Anywhere Enterprise. Igualmente importante, principalmente quando trata-se da adesão aos princípios essenciais de privilégios menores e separação de tarefas, é o suporte para Controle de acesso otimizado baseado em função ou RBAC.

Há cinco funções distintas (consulte **Tabela 1**) para considerar dentro da arquitetura básica e principais funções da plataforma da RPA. Criadores de bot utilizam o Bot Creator para capturar lógica empresarial e para criar automações correspondentes. Criadores de bot trabalham com aplicativos de teste e conjuntos de dados para que os sistemas de produção não sejam impactados durante a fase de desenvolvimento. Um bot individual geralmente passará por muitas interações e versões diferentes, não apenas durante o desenvolvimento inicial, mas também sempre que processos e/ou aplicativo de destino empresariais associados forem atualizados. Os Verificadores de bot também trabalham com o Bot Creator para testar bots com relação a desempenho, integridade de dados e segurança, garantindo que cada bot realize sua tarefa específica de forma segura. Verificadores de bot funcionam como um segundo estágio de autorização para o bot, antes dele poder ser executado com aplicativos e dados de produção.

Depois do bot ser testado e tiver passado por uma revisão de segurança, o Promotor de bot trabalha com os Criadores/Verificador de bot para designar a versão do bot que deve ser usada na produção. Esta é a única versão do bot que estará visível para o Operador de bot, que coordena com as unidades empresariais para agendar e executar o bot. O Operador de bot também é responsável pelo monitoramento do desempenho de bot dentro do Control Room, incluindo a solução de quaisquer problemas relacionados ao tempo de execução que aparecerem. Por fim, a responsabilidade para a administração geral da plataforma, incluindo componentes de configuração, interfaces e todas as outras funções/permissões, se encaixam na administração da RPA.

Separação avançada de tarefas

Esse conjunto central de funções demonstra um ponto de início básico de RBAC, mas uma separação ainda maior de tarefas é possível dentro da plataforma Automation Anywhere Enterprise. Usando o assistente de criação de função integrado, os administradores podem definir facilmente funções personalizadas e privilégios/permissões que são responsáveis pelo pacote completo dos objetos e funções do Control Room, incluindo gerenciamento de usuário, licenciamento, Cofre de credenciais, conjuntos de Bot Runners, agendamentos de bot, operações/dashboards de bot e logs de auditoria. Conforme cada privilégio é selecionado, o assistente adicionará, de forma dinâmica, etapas para privilégios eventual/privado.

Por exemplo, quando BOTS > Exibir meus bots > Executar Meus privilégios de bots são selecionados (consulte **Figura 5**), o fluxo de trabalho adicionará uma etapa para indicar as Pastas de bot específicas (ou seja, conjuntos de bots) para qual o acesso está sendo cedido. O resultado é a habilidade de estabelecer funções altamente leais com controles de acesso otimizados suficientemente para atender às necessidades dos ambientes mais rigorosos, seguros e regulamentados para conformidade.

Função	Descrição
Administrador da RPA	Administra o sistema (configurando componentes, funções, interfaces)
Bot Creator	Um especialista de processo empresarial que cria bots com o Editor de tarefas e realiza testes funcionais básicos
Verificador de bot	Um verificador de garantia de qualidade que revisa os bots com relação a precisão funcional, desempenho e segurança
Promotor de bot	Um administrador que aprova e move bots entre estágios de desenvolvimento, teste e produção
Operador da RPA	Um operador que agenda, executa e monitora o desempenho dos bots

Tabela 1: Principais funções de RPA no Automation Anywhere Enterprise

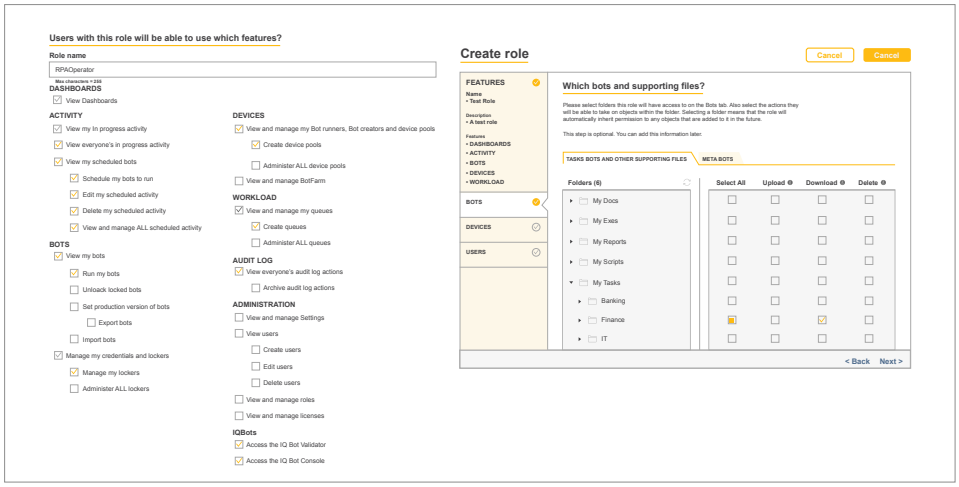

Figura 5: Criação de função com autorização otimizada

Painéis de controle independentes

Além dos recursos de RBAC extensos, o Automation Anywhere Enterprise realiza, de forma inerente, a separação lógica de tarefas implantando uma arquitetura que separa por completo as tarefas de desenvolvimento e execução de bot.

Os Bot Creators só podem carregar e baixar bots para o e do sistema de controle da versão dentro do Control Room. Ao mesmo tempo, os Bot Runners são limitados a executar bots; eles não têm acesso à criação de bot e funcionalidade de teste. Essa separação imposta de forma arquitetônica de tarefas constitui uma autorização dupla consistente com as melhores práticas do National Institute of Standards and Technologies (NIST), pois ela requer (no mínimo) um usuário desenvolvedor e empresarial para habilitar, por fim, uma automação de processo empresarial.

Domínios de processamento independente

Um caso de uso poderoso dos recursos de RBAC da plataforma, principalmente para grandes empresas, é o estabelecimento de domínios de processamento independentes (consulte **Figura 6**). Isso pode ser realizado com organização/armazenamento rigoroso de bots para cada domínio desejado em uma pasta correspondente dentro do Control Room.

Caso em questão: Bots associados com aplicativos de finanças seriam colocados em uma pasta de finanças, enquanto aqueles associados com RH seriam colocados em pasta de RH. Operadores de bot do departamento financeiro receberiam privilégios apenas para bots financeiros e Bot Runners financeiros; Operadores de bot para RH receberiam privilégio apenas para bots e Bot Runners de RH, e assim por diante, para outros domínios de processamento/automação (consulte **Figura 6**).

O resultado é a separação adicional de tarefas e isolamento de aplicativos e dados associados, esse momento no nível de UO/domínio, pois operadores individuais não conseguem ver ou operar bots fora de determinado domínio.

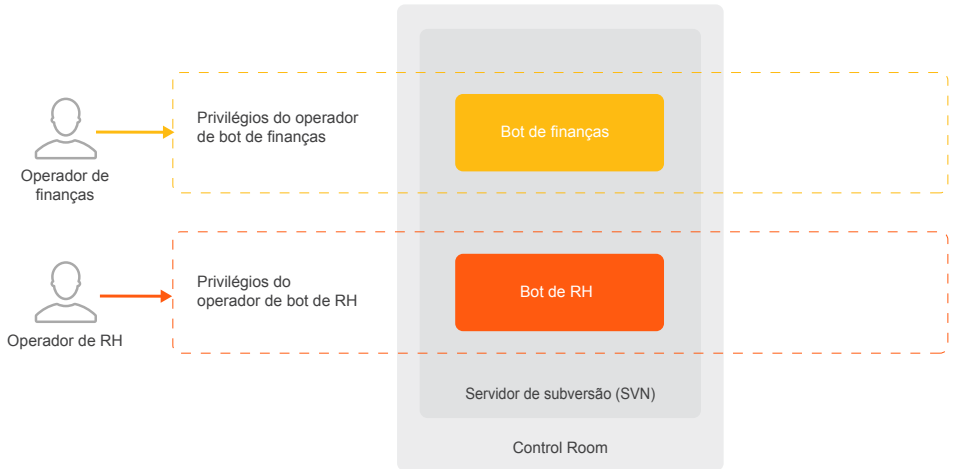

Figura 6: Suporte para domínios de processamento independente

PROTEÇÃO DE DADOS DE PONTA A PONTA

Autenticação multicamada e controle de acesso otimizado são essenciais para um ambiente de controle rigoroso. O mesmo acontece com a proteção de ponta a ponta, que também é necessária para manter a confidencialidade e integridade de processos empresariais críticos, dados sensíveis e segredos relacionados (por exemplo, credenciais).

A plataforma Automation Anywhere Enterprise aborda essa necessidade com um Cofre de credenciais integrado e fornece um conjunto extenso de proteções que não só protegem dados em repouso quanto em trânsito, mas também enquanto estiver em uso em sistemas individuais.

Chaves de criptografia e o Cofre de credenciais

A **Figura 7** exibe as principais chaves de criptografia usadas pela plataforma, juntamente com seu relacionamento com o Cofre de credenciais. Toda criptografia é realizada usando módulos criptográficos FIPS 140-2 validados de Nível 1.

Durante a instalação (a parte à esquerda da **Figura 7**), o sistema gera um par de chaves públicas/privadas RSA de 2048 bits e uma chave AES de 256 bits. A chave privada do par RSA 2048 é conhecida como o Comando principal, enquanto a chave AES 256 é conhecida como Chave de dados. O Comando principal é apresentado ao administrador de instalação para manter a segurança em um local seguro fisicamente fora do sistema. A chave pública é usada para criptografar a Chave de dados. Tanto a chave pública quanto a Chave de dados criptografada são armazenadas no banco de dados. Quando estiverem em uso, todas as chaves e dados criptografados estão posicionados na memória segura criptografada usando a API do Microsoft Data Protection (DPAPI).

Durante inicialização ou reinicialização do Control Room (lado direito da **Figura 7**), o administrador recebe um aviso para fornecer o Comando principal. A Chave de dados criptografados é recuperada do banco de dados e descriptografada usando o Comando principal. A Chave de dados agora está pronta para uso. Como o sistema armazena e recupera dados do Cofre de credenciais, a Chave de dados é usada para criptografar e descriptografar esses dados.

O Cofre de credenciais é usado para armazenar todas as credenciais gerenciadas do sistema e dados de configuração de sistema críticos. Ele também pode ser usado para armazenar outros dados sensíveis (por exemplo, pares de nome-valor) usados nas automações de uma organização. Como um resultado, Criadores de bot podem evitar a prática insegura de credenciais pesadas e outros argumentos/dados sensíveis diretamente dentro de suas automações.

Proteção de dados em repouso

Além de criptografar credenciais locais e selecionar dados de tempo de execução usados por bots, o Cofre de credenciais fornece armazenamento seguro para parâmetros de configuração sensível e detalhes com relação ao controle de versão integral e serviços de e-mail.

Proteção de dados em trânsito

Todos os serviços de rede de clientes e do Control Room usam Transport Layer Security (TLS) 1.2 para garantir dados de segurança e integridade durante transporte entre componentes.

Credenciais usadas para autenticação de Bot Creator/Runner para o Control Room são criptografados antes de serem enviados por uma conexão TLS segura. Essa camada extra de criptografia não protege apenas contra problemas de empilhamento de rede (como com Heartbleed), mas também previne a exposição de credenciais para implementações onde a conexão de TLS da camada externa é encerrada no balanceador de carga de front-end.

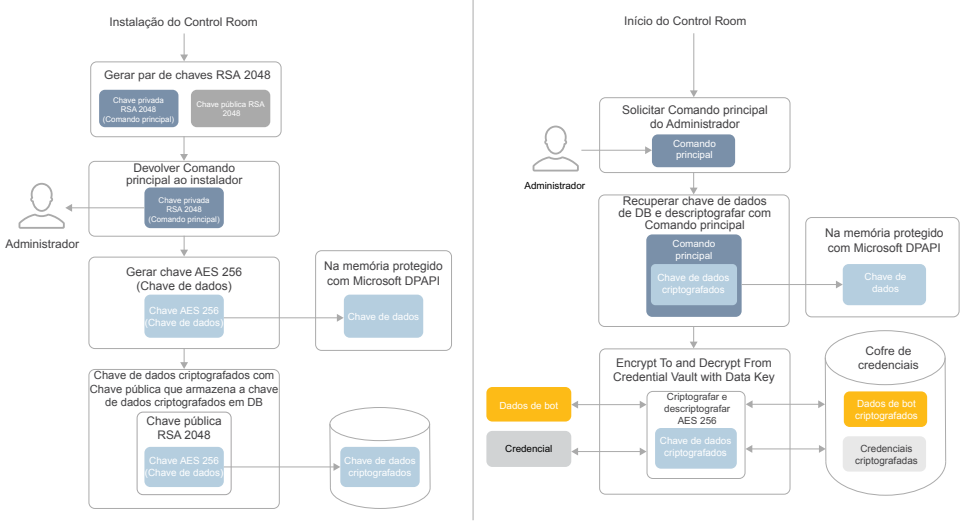

Figura 7: A arquitetura de criptografia do Automation Anywhere Enterprise

Proteção de dados em uso

A segurança de tempo de execução começa com proteção de credencial distribuída. Especificamente, não há armazenamento de credencial local nos Bot Runners. Credenciais e outros dados recuperados dinamicamente do Cofre de credenciais para uso dentro das automações são retidos apenas em formato criptografado em memória volátil, e são apagados depois que o bot associado termina sua execução.

Outros recursos e opções de configuração que podem ser usados para prevenir acesso não autorizado para informações confidenciais (ou seja, vazamento de dados) ou manipulação com bots durante o tempo de execução, incluem:

+ Modo oculto – onde nenhuma janela de programa é exibida na tela local e os usuários logados têm a opção de desabilitar a captura de imagem de Bot Creators e Bot Runners, prevenindo assim informações sensíveis exibidas na tela em vez de serem armazenadas em bots
+ Bloqueio de entrada – a habilidade de desabilitar o mouse e teclado da máquina onde a automação está sendo executada
+ Limite de tempo – a habilidade de definir um limite de tempo após o qual uma automação será encerrada se sua execução ainda não tiver terminado
+ Controle central – a habilidade de controlar centralmente (por exemplo, pausar, retomar, parar) a operação de automações sendo executadas remotamente dentro do Control Room

SUPORTE DE CICLO DE VIDA DE DESENVOLVIMENTO DE SOFTWARE SEGURO (SDLC)

Para maximizar os controles e proteções posicionadas no ambiente de automação, o cenário de implantação básico descrito anteriormente pode ser "expandido" para entrega adicional nas melhores práticas do Secure Software Development Lifecycle (SDLC), como aqueles necessários para FISMA, FedRamp e PCI DSS. O modelo de implantação avançado resultante fornece três zonas de RPA distintas, uma para desenvolvimento, uma para teste de aceitação de usuário (UAT) e uma para produção (consulte Figura 8). Cada zona é logicamente separada (isolada) com grupos de usuário diferentes com funções e privilégios distintos. As linhas verticais tracejadas representam segmentação e firewalls de rede.

Como no modelo de implantação básico, o ciclo de vida do bot se inicia no desenvolvimento. Quando os Criadores de bot estão satisfeitos com o bot, Promotores de bot de UAT transferem o bot do repositório de versionamento de desenvolvimento (SVN) para o repositório de UAT. O objetivo exclusivo da zona UAT é testar os bots com relação a precisão, desempenho e segurança. Depois que o bot passar no teste de aceitação, um Promotor de bot de produção o transfere para a zona de produção. Neste ponto, ele obtém o status de produção e torna-se disponível para Operadores da RPA para uso sem aplicativos de produção. Em cada etapa no processo, verificações e certificações são realizadas por administradores distintos com funções e privilégios diferentes. Separação rigorosa de tarefas e controles multicamadas são integrados por design para garantir que a força de trabalho digital é confiável, escalável, eficiente, segura e compatível.

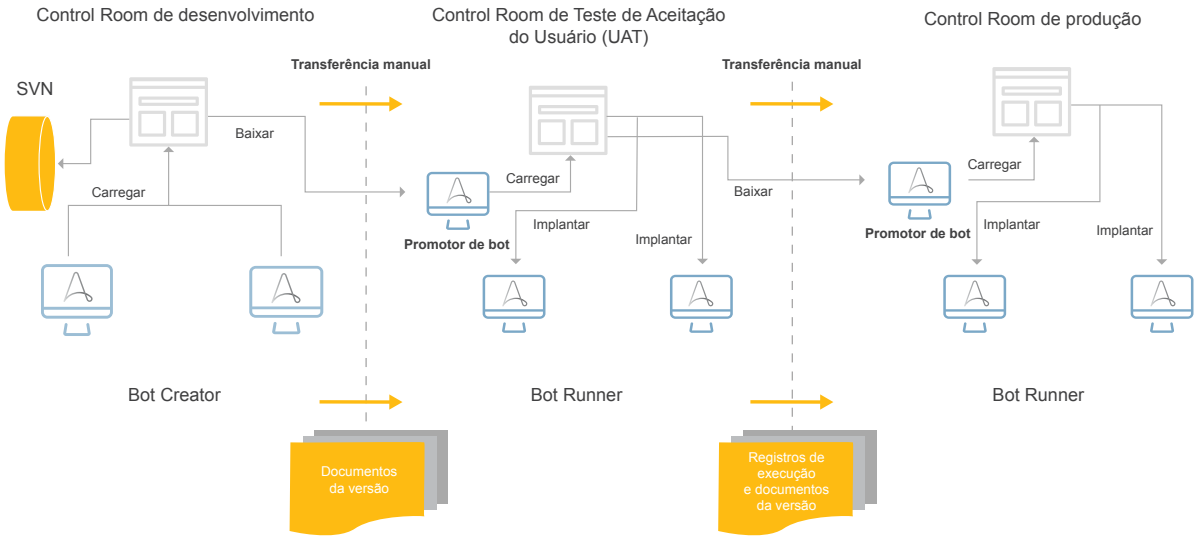

Figura 8: Modelo de implantação avançado para suporte de SDLC completo

LOGON E MONITORAMENTO

Recursos de log de auditoria abrangente, monitoramento e relatórios são componentes essenciais da arquitetura de segurança para qualquer solução importante de TI. Automation Anywhere Enterprise não é uma exceção.

Na plataforma, detalhes de evento (quem, o quê, quando, onde e o resultado) são capturados automaticamente sobre mais de 60 tipos de ações de usuário/entidade, incluindo a criação, modificação, ativação, desativação e remoção de usuários, bots, Bot Creators e Bot Runners. A segurança é alcançada por meio de uma combinação de captura automática, vinculação de cada atividade a uma identidade específica e uma política padrão de somente leitura. Em primeiro lugar, o RBAC também pode ser implantado para controlar rigorosamente quais funções têm visibilidade aos logs de auditoria.

De uma perspectiva de monitoramento, painéis automatizados e relatórios são acessíveis dentro do Control Room e podem ser personalizados para identificar e alertar atividades anormais (ou qualquer outro detalhe que a equipe de automação ou segurança decidir ser de interesse). Além disso, a habilidade de exportar logs possibilita o uso de outras análises, relatórios e infraestrutura de investigação/resposta de incidente já em uso pela organização, como SIEM, UEBA e ferramentas de análise avançadas.

FUNCIONALIDADES DE SEGURANÇA E RESILIÊNCIA ADICIONAIS

Automation Anywhere Enterprise oferece suporte adicional à segurança empresarial e objetivos de resiliência com:

+ Uma arquitetura de componente distribuída (e flexível) que é capaz de se encaixar perfeitamente a uma infraestrutura e processos de alta disponibilidade/recuperação de desastre (HA/DR) existente da organização
+ Um sistema de controle de versão integral (Apache Subversion) que, em conjunto com os recursos RBAC extensivo da plataforma, é possível implementar e aplicar uma política e processos de gerenciamento de mudança altamente rigorosos
+ Ferramentas como as estruturas de Hibernate e ReactJS durante o desenvolvimento de código de plataforma para ajudar a eliminar a suscetibilidade para ataques comuns (como Inserção de SQL e Scripts entre sites)
+ Um protocolo/plano de segurança para desenvolvimento de código que requer multiferramentas contínuas, rastreamento multicamadas para detectar e eliminar vulnerabilidades de software

Mais detalhes sobre esses e os muitos outros controles, proteções e recursos de segurança que fazem parte do Automation Anywhere Enterprise podem ser encontrados aqui: Automation Anywhere Enterprise: Arquitetura de segurança.

A Automação Robótica de Processos apresenta uma grande promessa para empresas modernas que procuram diminuir seus custos operacionais, aumentar a satisfação do cliente e ganhar uma vantagem com relação à concorrência. Como líder de mercado, a plataforma de força de trabalho digital inteligente, Automation Anywhere Enterprise ajuda a garantir o máximo de conquistas desses e de outros benefícios, entregando recursos não apenas de confiabilidade, escalabilidade e usabilidade necessários para o sucesso, mas também segurança de nível empresarial necessária para preservar a confidencialidade, integridade e disponibilidade de todo o ambiente de automação.

Para obter mais informações sobre o Automation Anywhere Enterprise, acesse: https://www.automationanywhere.pt/products/enterprise