ForgeRock

LINHA INTELLIGENT ACCESS

Introdução

Intelligent Access da ForgeRock

Visão Geral

A segurança moderna exige que as empresas se protejam contra vazamentos de dados de qualquer local e de qualquer tipo de usuário: seus próprios funcionários, parceiros, clientes e coisas conectadas à Internet. Para lidar com esses riscos, o modelo de segurança **Análise Contínua e Adaptável de Riscos e Confiança (CARTA)**[1] do Gartner recomenda que as empresas adotem uma prática de gerenciamento de acesso que permita visibilidade e avaliação contínuas das decisões de segurança, estabelecidas por meio de múltiplos atributos, utilizando os *insights* mais amplos e profundos para avaliar os riscos de usuários interagirem com seus canais digitais.

O modelo de **Zero Trust**[2] da Forrester sugere que não há redes, usuários, dispositivos, sessões, dados ou serviços inerentemente confiáveis (em comparação com não confiáveis). A confiança deve ser concedida com base em múltiplos sinais contextuais, comportamentais e baseados em risco. Não é mais suficiente utilizar autenticação de um ou dois fatores, mesmo que sejam fatores fortes. Sinais adicionais baseados em contexto, comportamento e risco (autenticação adaptativa) também devem ser considerados.

Como líder em Gerenciamento de Identidade e Acesso (IAM) em sua empresa, é fundamental que você considere como incorporar esses princípios de CARTA e Zero Trust enquanto continua a oferecer as experiências de usuário seguras e sem atrito que seus clientes esperam.

Neste informe, você aprenderá sobre os recursos e benefícios do Intelligent Access da ForgeRock, incluindo jornadas do usuário, nós e a Trust Network. O Intelligent Access da ForgeRock é o único mecanismo dinâmico de orquestração e inteligência do mundo que permite projetar e gerenciar jornadas de usuário seguras e contínuas para todos os seus aplicativos e serviços.

> Sem escrever uma única linha de código, você pode usar a interface de arrastar e soltar do Intelligent Access para projetar, configurar, medir e ajustar múltiplas jornadas do usuário.

O Intelligent Access usa sinais digitais que fornecem informações contínuas sobre o dispositivo, contexto, comportamento, escolhas, análises e riscos do usuário. Os Kits de Desenvolvimento de Software (SDKs) da ForgeRock fornecem informações e dados ainda mais aprofundados sobre os dispositivos que acessam seus sistemas, para que você possa definir políticas de autorização e acesso dinâmicos e granulares.

Com o Intelligent Access, você obterá uma visibilidade profunda de como as pessoas e os dispositivos interagem com seus aplicativos e serviços. Isso ajudará você a aumentar a segurança, aprimorar a experiência do usuário e fornecer personalização dinâmica.

Recursos Expandidos

O Intelligent Authentication da ForgeRock agora é conhecido como Intelligent Access. O nome foi alterado para refletir um conjunto de recursos que vai além da autenticação para incluir funcionalidades adicionais. Iremos explorar esses recursos com mais detalhes em informes subsequentes. Os recursos estendidos do Intelligent Access incluem:

- **ForgeRock Go:** A implementação do padrão FIDO2 WebAuthN da ForgeRock permite que usuários e dispositivos se cadastrem e autentiquem sem nomes de usuário e senhas.
- **Autoatendimento Inteligente:** Novos recursos facilitam a criação de jornadas para os usuários para que eles possam gerenciar suas próprias preferências de cadastro, redefinições de senha via autoatendimento, recuperação de conta, criação de perfil progressiva e gerenciamento de perfil.
- **Antifraude:** Se o seu objetivo é reduzir o custo total da fraude (TCOF), você pode avaliar os fatores de risco e detectar o acesso fraudulento utilizando árvores de Intelligent Access, que se integram à soluções antifraude de terceiros oferecidas em nosso Trust Network da ForgeRock. Você pode combinar essas integrações com os recursos de autorização transacional da ForgeRock para mitigar transações fraudulentas e reduzir o custo operacional total de propriedade.
- **Identidade Segura para Internet das Coisas (IoT):** Esse recurso suporta gerenciamento de identidade e jornadas de acesso para dispositivos conectados à Internet (“coisas”). Ele oferece integração flexível para coisas inteligentes e restritas no Intelligent Access e completo gerenciamento do seu ciclo de vida de identidade – provisionamento, ativação, desativação e descarte.

Projete Jornadas de Usuário Poderosas

Na base do ForgeRock Intelligent Access está sua interface visual de arrastar e soltar que permite projetar jornadas de usuário modulares, orquestradas e personalizadas conhecidas como "árvores". Sob a superfície de nossas configurações de arrastar e soltar, está a plataforma de IAM mais abrangente e poderosa do setor.

Árvores

Uma jornada do usuário é o início, meio e fim das interações de um usuário com seus sistemas. Ela pode começar com uma página de login ou cadastro e continuar através de várias interações com seu repositório de identidades, site e aplicativos. A ForgeRock chama essas jornadas de "árvores" porque uma jornada do usuário pode se ramificar em múltiplos caminhos e pontos de decisão.

> Uma árvore criada no Intelligent Access é a representação visual de uma jornada do usuário.

As árvores do Intelligent Access suportam jornadas de usuários para muitos casos de uso de negócios diferentes, incluindo cadastro de usuários, autenticação e autoatendimento. Uma árvore de cadastro solicita que um usuário crie uma conta, defina suas credenciais padrão, cadastre dispositivos e defina múltiplas preferências. Uma árvore de autenticação coleta credenciais, verifica essas credenciais em relação a um repositório de identidades e define os resultados de aprovação/reprovação. Uma árvore de autoatendimento permite que os usuários solicitem uma redefinição de senha, gerenciem suas próprias informações de perfil e definam seus dispositivos preferenciais. O Intelligent Access fornece muitas árvores pré-construídas que podem ser personalizadas ou usadas "*as-is*" (ou como estão).

Nós

Os nós do Intelligent Accesss são pequenas unidades de trabalho que compõem uma jornada do usuário. Cada nó tem um único propósito: definir ações específicas realizadas durante a jornada do usuário. O Intelligent Access da ForgeRock possui muitos nós pré-programados que detectam sinais digitais, tomam decisões e direcionam a jornada do usuário. É possível combinar nós para coletar sinais que você configura no Intelligent Access para determinar se os níveis de acesso de um usuário devem ser modificados durante uma sessão. Esses sinais são armazenados em um token de sessão que fornece informações sobre a sessão do usuário para aplicativos downstream.

O seguinte é um exemplo de como você pode construir uma jornada do usuário: Um nó coleta um nome de usuário, enquanto outro envia uma notificação push para um dispositivo. Outro nó retirado da Trust Network da ForgeRockchama um serviço de detecção de fraude de terceiros para informá-lo sobre a autenticidade e a segurança do usuário e suas ações durante a sessão.

Você pode conectar esses nós em uma ordem lógica na ferramenta de design visual do Intelligent Access, como faria usando o software de fluxograma. Você pode criar experiências sofisticadas e adequadas para uso vinculando nós, criando loops e inserindo nós na árvore.

Tipos de Nós

O Intelligent Access possui vários nós integrados que estão incluídos na plataforma:

- **Os Nós de Autenticação Básica** são usados para funções básicas de jornada do usuário, como coletar nomes de usuário e senhas, além de nós de decisão para autenticação em repositório de identidades, como LDAP e Kerberos, para acesso único (SSO) de desktop.
- **Os Nós de Autenticação Multifator** são usados para projetar árvores com recursos de autenticação multifator, como autenticação da Web sem senha e autenticações push.
- **Os Nós Comportamentais** ajustam o comportamento das árvores de autenticação. O nó de aumentar a contagem de login trabalha com o nó de decisão de contagem de login para acionar uma ação quando a propriedade de contagem de login bem-sucedido de um usuário atinge um número especificado. Por exemplo, você pode definir a contagem de login como “5” e ordenar que o nó de decisão de contagem de login falhe após cinco tentativas de autenticação incorretas.
- **Os Nós de Gerenciamento de Risco** examinam o risco encontrado associado à autenticação e agem em resposta. Existem nós para aumentar ou diminuir o nível de autenticação atual, comparar o valor do nível de autenticação atual com um valor configurado ou adicionar suporte CAPTCHA às árvores de autenticação. Um nó de bloqueio de conta bloqueia ou desbloqueia o perfil de conta do usuário que está tentando a autenticação. Use este nó de bloqueio como o resultado final de uma "falha" no nó de decisão de contagem de login.
- **Os Nós de Autenticação Contextual** examinam o contexto de uma autenticação e reagem de várias maneiras – como coletar e validar certificados e coletar, combinar e armazenar metadados sobre o dispositivo com o qual o usuário está tentando a autenticação.
- **Os Nós de Dispositivo** são novos no Intelligent Access e são sensíveis ao contexto. Eles identificam os dispositivos dos quais o usuário faz login, armazenam perfis de dispositivos para autenticação sem senhas, associam um dispositivo a um local conhecido, definem cercas geográficas ao redor de um dispositivo e notificam o sistema se o dispositivo foi comprometido. Os SDKs móveis ou da Web do Intelligent Access da ForgeRock detectam a limpeza do dispositivo (por exemplo: se um dispositivo está usando o sistema operacional mais recente ou “jailbreak” foi realizado) e anomalias como distância de viagem impossível entre o local onde ocorre uma tentativa de login e a localização de um dispositivo confiável de segundo fator.

Por exemplo, ele detectará que uma tentativa de autenticação foi feita em uma rede pública de uma cafeteria em Las Vegas e que o dispositivo móvel cadastrado do usuário está com o usuário em Cingapura, fazendo com que o acesso autorizado seja improvável.

- **Os Nós de Autenticação de Federação** fornecem árvores com recursos de federação, como OAuth 2.0, autenticação social OpenID Connect, SAML2 e provisionamento de contas.
- **Os Nós de Autenticação de Gerenciamento de Identidade** executam tarefas de gerenciamento de identidade durante a jornada do usuário, como mapear usuários anônimos para uma sessão, coletar preferências do usuário para autenticação e definir preferências para autenticação social.
- **Os Nós de Autenticação de Utilidade** incluem vários utilitários (tarefas) que são acionados em uma jornada do usuário, como enviar um e-mail de verificação para o usuário. Você também pode criar nós de página que combinam múltiplas tarefas em uma única página, como exigir que um usuário insira seu nome de usuário e senha e escolha um fator de autenticação multifator (MFA).
- **Nós para IoT:** O ForgeRock oferece suporte à autenticação e cadastro de IoT, incluindo dispositivos IoT, serviços de IoT e um Gateway IoT.

Muitos nós adicionais estão disponíveis no Trust Network da ForgeRock e no Marketplace da ForgeRock que foram projetados por parceiros e outros colaboradores.

Construindo uma Àrvore Simples

Os blocos de construção básicos de uma árvore de autenticação incluem o seguinte:

- Um **nó de coleta de credenciais** – por exemplo, para nome de usuário e senha, biometria ou token de hardware. Use um Nó de Página para combinar nós de coleta de credenciais para que o usuário veja todos os elementos em uma única página.
- Um **nó de decisão** para verificar a validade da tentativa de autenticação. Por exemplo, um nó de decisão do repositório de dados pode verificar um nome de usuário e uma senha em um diretório. Outro nó pode verificar o tipo de navegador, se um limite de política foi atendido e outros fatores.
- Um **resultado** definido como sucesso/fracasso, verdadeiro/falso – ou resultados mais arbitrários e dinâmicos.

Abaixo há um exemplo de uma árvore de autenticação com nós para coletar nome de usuário e senha. O nó de decisão do repositório de dados com resultados Verdadeiro e Falso permitirá o acesso do usuário se ele autenticar com sucesso no repositório de dados ou retornará à página de nome de usuário e senha se a autenticação falhar.

Figura 1: Uma árvore de autenticação simples

Você pode seguir um processo semelhante para projetar árvores de autenticação, cadastro e autoatendimento mais complexas. Você pode encontrar muitas árvores de exemplo na documentação, por meio da Trust Network e das contribuições do Marketplace de usuários da ForgeRock.

Vantagens de Usar o Intelligent Access para Construir Jornadas do Usuário

A estrutura de árvores do Intelligent Access protege a autenticação da sua empresa e as jornadas do usuário de acesso. Suas equipes podem projetar uma interação consistente do usuário em aplicativos modernos e legados e unificar silos de identidade. Você pode obter mais visibilidade de como os usuários interagem com seu ambiente para oferecer personalização dinâmica e redução de risco direcionada em todas as etapas – desde cadastro, autenticação, autoatendimento do usuário e gerenciamento de opções de privacidade e consentimento. As árvores do Intelligent Access podem atender a praticamente qualquer requisito de autenticação e acesso relacionado aos negócios.

Apenas alguns dos benefícios adicionais do Intelligent Access estão listados abaixo, juntamente com algumas árvores de exemplo para casos de uso específicos. Observe que quaisquer árvores de exemplo são representações de como você pode configurar uma jornada do usuário. Lembre-se de que você provavelmente precisará fazer alguns ajustes para atender aos requisitos específicos do seu ambiente e casos de uso.

Economize Tempo e Esforço

As árvores do Intelligent Access são uma estrutura para criar jornadas do usuário "com cliques, não com código" para a maioria dos casos de uso. Em vez de projetar jornadas de usuário por aplicativo, você pode projetar jornadas uma única vez e habilitá-las globalmente. Os clientes relatam que estão projetando cada jornada do usuário em uma única sessão, em vez de passar semanas criando código, testando e refazendo o código das várias integrações.

Reduza o Atrito do Cliente e as Taxas de Abandono

O Intelligent Access da ForgeRock reduz o atrito que os clientes e funcionários experienciam com o cadastro e a autenticação de contas. Muitas vezes, os usuários que tentam iniciar uma avaliação de um serviço encontram uma página de cadastro longa e, por fim, abandonam o site. Com o Intelligent Access, você pode criar árvores de cadastro simples e eficientes que permitem aos usuários que acessem o que desejam e coletam informações sobre a experiência do usuário.

O Intelligent Access da ForgeRock leva em consideração todo o contexto de como um usuário interage com o sistema e monitora o acesso continuamente.

Mesmo antes da autenticação inicial, o Intelligent Access determina vários atributos do usuário, executa cálculos de risco contínuos e altera o nível de acesso ou aciona etapas de autenticação adicionais para que o usuário execute para transações de alto risco. Ao reduzir o atrito e aumentar a segurança com o Intelligent Access, você pode:

- Conhecer seu público e criar jornadas de usuário excepcionais em todas as etapas do ciclo de vida do usuário.
- Proporcionar aos clientes uma jornada de login menos intrusiva, aprimorando a sua relação com o serviço.
- Aproveitar um único modelo de autenticação e acesso para todos os sistemas.
- Usar inteligência artificial (IA) integrada para criar o modelo da sessão do usuário e remover mais atritos à medida que a confiança na sessão do usuário aumenta.

Exija Autenticação Avançada Quando Necessário

Um pouco de atrito extra pode ser bom – e é algo que os usuários esperam. O Intelligent Access requer autenticação avançada quando necessário. Por exemplo, se um usuário funcionário não fez login recentemente, excluiu seu histórico de cookies, está fazendo login de um local ou rede diferente ou perdeu seu notebook ou dispositivo móvel, ele deve fornecer autenticação adicional antes de receber acesso aos recursos corporativos. Sem houver um sinal de confiança conhecido, uma tentativa de autenticação ou acesso tem grandes chances de ser de um invasor.

O Intelligent Access foi projetado para configurar sinais de confiança para contas de usuários e permitir que os usuários escolham e controlem como se cadastram e autenticam. Durante o cadastro de autoatendimento, os usuários podem escolher qual método de MFA usar. Habilitar a escolha ajuda a reduzir qualquer atrito percebido porque os usuários se envolvem em sua própria segurança.

A árvore na **Figura 2** oferece ao usuário cinco opções de MFA. Dependendo da opção selecionada, os nós subsequentes são ativados até que um Sucesso ou Falha de autenticação seja gerado.

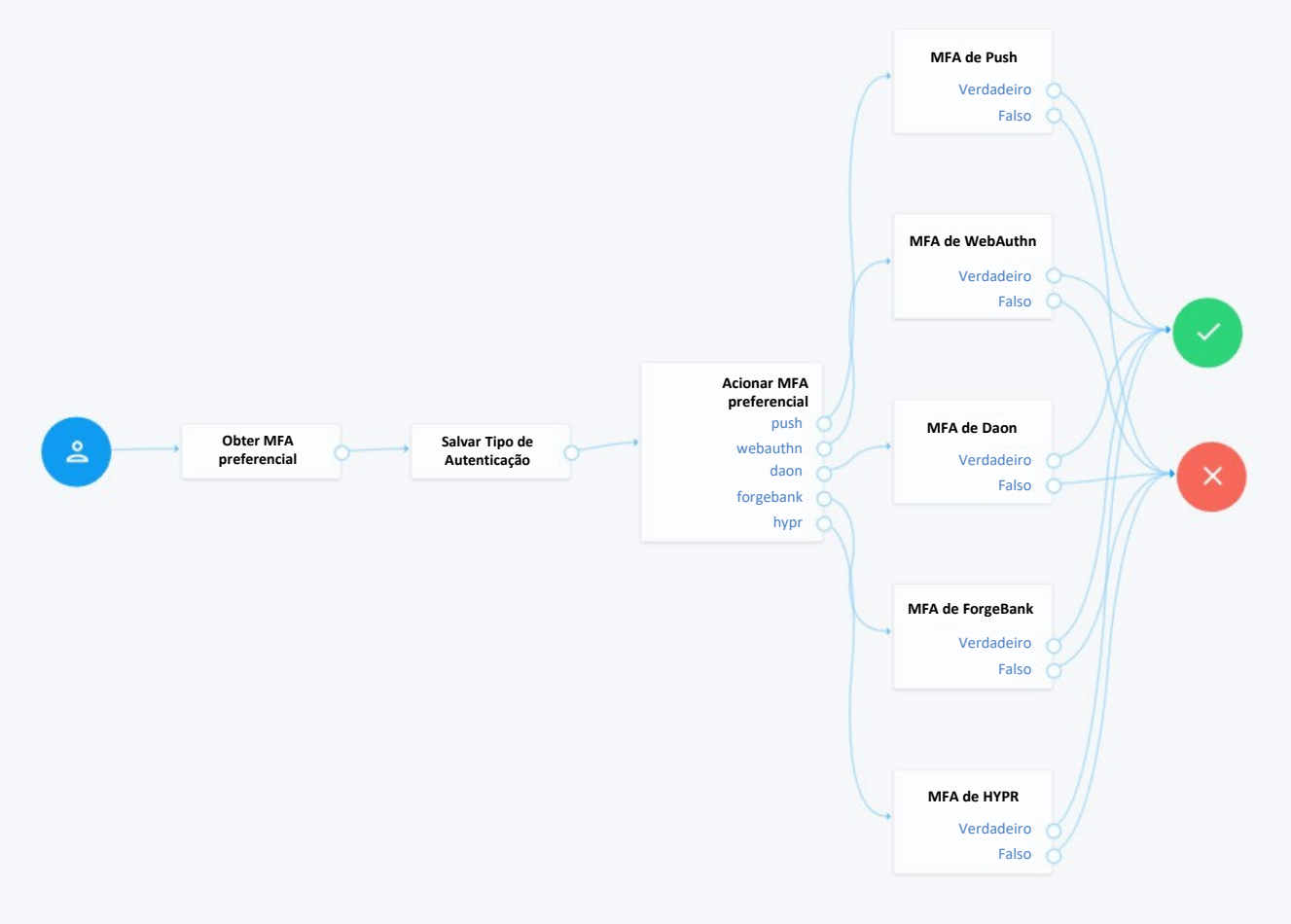

Figura 2: Uma árvore de autenticação avançada

Analise os Atributos de Login do Usuário

O Intelligent Access inclui ferramentas de análise de login do usuário que você pode usar para projetar múltiplas jornadas de autenticação e testar a eficácia de cada uma delas. Ao analisar como os usuários se autenticam, você pode criar jornadas do usuário que aumentam as taxas de adoção do usuário e melhoram a experiência do cliente, além de redirecionar automaticamente usuários suspeitos para monitoramento adicional.

Na **Figura 3**, um nó de decisão de endereço IP captura os endereços IP dos usuários quando eles efetuam login. Você pode configurar intervalos de endereços IP para bloquear e impedir a autenticação de usuários com esses endereços IP de origem.

O terceiro nó à direita captura a autenticação com base na região geográfica dos usuários. Em seguida, um nó conta o número de logins de cada região geográfica e se o login é de um dispositivo móvel. O Nó Coletor de Navegador verifica os tipos de navegador e define os nós de decisão para marcar os navegadores como confiáveis ou não confiáveis.

Todas essas informações são armazenadas em um token de sessão que os aplicativos downstream podem usar para decidir se aceitam ou não o tráfego com base em qualquer um desses critérios. Esses sinais melhoram a segurança e também podem otimizar as experiências do usuário (por exemplo: usuários que fazem login da Espanha usando um dispositivo móvel, são redirecionados para páginas em espanhol otimizadas para dispositivos móveis).

Figura 3: Análise de login do usuário

Aprimore os Acordos de Nível de Serviço

O Intelligent Access facilita a conformidade com acordos de nível de serviço (SLAs) para serviços de terceiros medindo o tempo que leva para a jornada de login e o tempo que leva para o serviço responder.

Os nós de início do temporizador e interrupção do temporizador do Intelligent Access podem ser colocados em uma árvore de autenticação para medir o tempo de autenticação dos usuários.

Figura 4: Os nós do temporizador medem o tempo de autenticação para um usuário

Você pode inserir nós em uma subárvore para extrair informações, como de onde os usuários estão efetuando login, o número de abandonos de cadastro em comparação com autenticações bem-sucedidas e o tempo de autenticação de cada jornada. Você pode configurar dois fluxos diferentes como um teste A/B e enviar uma pequena porcentagem de tráfego para cada fluxo para analisá-lo quanto à usabilidade com diferentes públicos e regiões, latência, e muito mais. Você também pode expor os dados por meio de chaves de métrica.

O Intelligent Access permite projetar as melhores e mais robustas jornadas do usuário e aprimorá-las continuamente ao longo do tempo.

Figura 5: Chaves de métrica exibem dados do temporizador

Facilite a Autorização Transacional

A autorização transacional aprimora a segurança exigindo que um usuário execute autenticações adicionais sempre que desejar acessar um recurso protegido por uma política de autorização.

Você pode personalizar facilmente o fluxo de autenticação para incorporar múltiplos sinais e impor a autenticação avançada com base em um acionador de política. Diferente da elevação de privilégios, as autorizações transacionais concedem aos usuários acesso a um recurso protegido apenas uma vez. Cada autorização adicional requer outra autenticação.

As políticas de autorização podem ser acionadas contextualmente com base no que os usuários ou clientes definirem. Por exemplo, um cliente de banco pode configurar um limite de US$ 100 para pagamentos automatizados de contas online. Qualquer fatura abaixo desse valor é paga automaticamente, e qualquer fatura acima de US$ 100 aciona uma notificação push no dispositivo móvel do cliente para permitir ou negar a transação.

Em um cenário de funcionário, uma empresa pode exigir que um usuário responda a uma notificação push em seu dispositivo móvel antes de permitir que acesse aplicativos com dados confidenciais.

A figura abaixo mostra uma política de transação para usuários autenticados. A política invoca uma resposta de MFA com base na política de transferência definida pelo usuário. O script mostrado no campo Ambientes invoca uma árvore de autorização de transação que solicita um desafio de MFA. A política depende do limite definido pelo usuário, portanto, ela só acionará a árvore de autorização de transação (**Figura 7**) se o limite do usuário for excedido. Esse tipo de política de transações está alinhada com o princípio de CARTA de autenticação contínua e decisões de autorização refinadas.

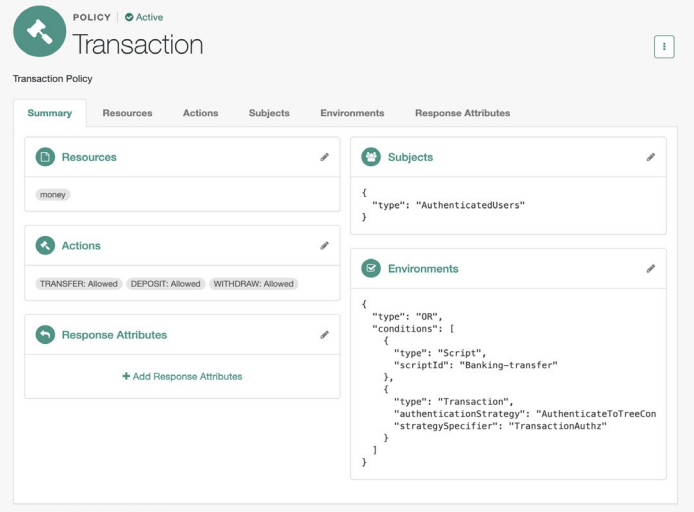

Figura 6: Política de transação para transferência bancária

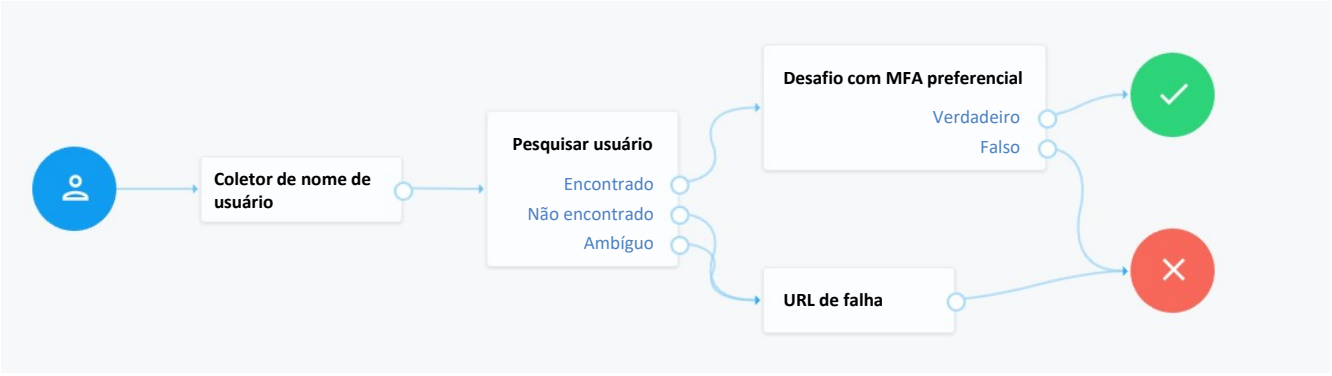

Figura 7: Desafio de autorização transacional com método de MFA preferencial

Aumente e Personalize as Jornadas do Usuário

A extensibilidade é um recurso chave da plataforma de identidade da ForgeRock. Embora você possa projetar a maioria das jornadas do usuário usando nós integrados e a interface do usuário (IU) de arrastar e soltar, inevitavelmente encontrará situações que exigem que você personalize jornadas para atender às suas necessidades de acesso específicas.

O Intelligent Access da ForgeRock oferece suporte para lógica empresarial personalizada com nós com script. Nós com script invocam scripts leves que chamam serviços baseados em REST. Em muitos casos, isso é suficiente para integrar autenticações básicas. Por exemplo, uma seguradora pode precisar validar o número da apólice de seguro de um usuário antes de autorizar uma transação. Você pode escrever um nó de decisão com script usando JavaScript ou Groovy que valide o número da apólice de seguro armazenado na sessão do usuário antes de autenticar o usuário. Você também pode integrar esses nós com script em seus aplicativos internos usando os SDKs da Web ou móveis da ForgeRock (iOS ou Android).

A **Figura 8** mostra um exemplo de como uma instituição de serviços financeiros pode escrever um script para capturar dados do dispositivo nativo quando um usuário se cadastra em seu serviço. A **Figura 9** mostra como esse Nó com script (segundo da esquerda) se encaixa em uma árvore de cadastro.

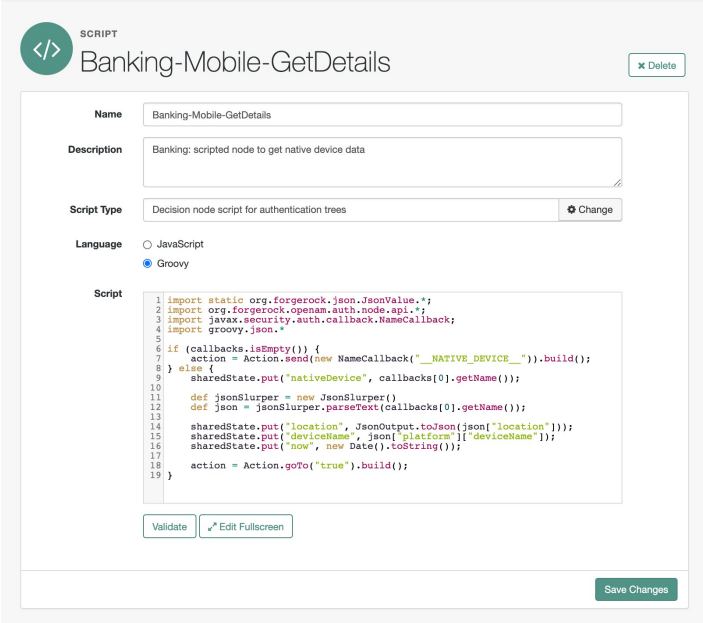

Figura 8: Script para capturar detalhes do dispositivo móvel

Para integrações mais profundas, com serviços de terceiros não padronizados ou sem suporte, você também pode escrever seus próprios nós personalizados para realizar validação de identidade, autenticação, avaliação de risco ou garantia.

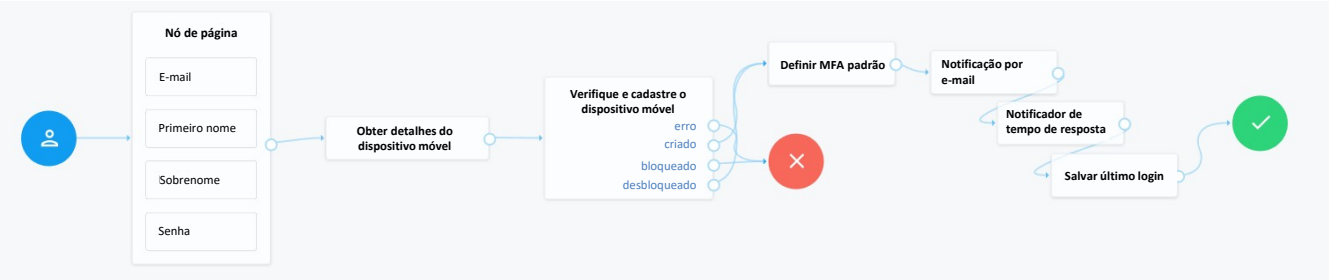

Figura 9: Exemplo de árvore bancária com nó com script

A Trust Network da ForgeRock

O Intelligent Access é fácil de usar, extensível e personalizável. Além dos nós, você pode acessar uma ampla variedade de soluções por meio do ecossistema de parceiros de tecnologia terceirizados da ForgeRock. Mais de 80 nós pré-integrados estão disponíveis na Trust Network da ForgeRock, já testados e validados pela ForgeRock, incluindo nós para autenticação forte, gerenciamento de fraude e risco, biometria comportamental e prova de identidade.

Além dos nós disponíveis com a plataforma da ForgeRock e da Trust Network da ForgeRock, há uma ampla variedade de nós de contribuição da comunidade disponíveis no Marketplace da ForgeRock. O Marketplace da ForgeRock é uma loja central para nós que não são enviados no produto, nem são parte da Trust Network.

Conclusão

O Intelligent Access da ForgeRock é uma plataforma de orquestração poderosa que possibilita projetar jornadas de usuário flexíveis que suportam decisões complexas e refinadas e incorporam múltiplos sinais e análises em todos os pontos da jornada do usuário.

O resultado é um cenário de segurança mais forte que mitiga fraudes e vazamentos de dados relacionadas à identidade, oferecendo acesso personalizado e sem atritos aos seus usuários.

[1] https://www.gartner.com/en/webinars/3891406/the-7-imperatives-of-continuous-adaptive-risk-and-trust-assessme

[2] https://go.forrester.com/blogs/category/zero-trust-security-framework-ztx/