ForgeRock®

LINHA INTELLIGENT ACCESS

Siga Sem Senha

Autentique com segurança.

Os problemas com senhas **2**
Autenticação forte **2**
Uma Abordagem à Autenticação Baseada em Padrões **3**
Tipos de autenticadores 4
Autenticação sem Senha ForgeRock **4**
Benefícios da autenticação sem senhas 4
Como Funciona a Autenticação sem Senha **5**
Usando autenticação sem senhas sem biometria 5
Configurando a Autenticação sem Senha **5**
Registrar um dispositivo 6
Habilitar a autenticação sem nome de usuário 6
Análise de um dispositivo 7
Alternativas de autenticação sem senhas 8
Quando usar a autenticação sem senhas 8
Conclusão **8**

Os problemas com senhas

Como profissional de gestão de identidade e acesso, você sabe que as senhas são um problema. Os seus usuários detestam ter de criar contas com elas. Suas equipes de segurança se preocupam com ataques de phishing por e-mail, roubo de credenciais e violações de dados.

O usuário médio tem mais de 90 contas. Lembrar senhas é difícil, e é por isso que mais de 50% dos usuários reutilizaram senhas em vários sites.[1] Criar senhas que dependem de informações pessoais torna as contas vulneráveis a ataques de dicionários. Usar um sistema de gestão de senhas é uma forma de lidar com o problema das senhas, mas alguns desses serviços em si são vulneráveis.[2]

> No "2021 Data Breach Investigations Report (DBIR)" da Verizon , 61% das violações envolveram credenciais.[3]

O ForgeRock Consumer Identity Breach Report 2020 descobriu que o acesso não autorizado era o método de ataque número um utilizado pelos criminosos cibernéticos para 43% das violações. Das indústrias inquiridas no relatório, o setor da saúde sofreu 34% de todas as violações, seguido dos serviços financeiros com 12%.[4]

Em 2018, o sistema de e-mail comercial da Iowa UnityPoint Health foi vítima de uma série de ataques de phishing por email, visando credenciais de funcionários. Embora o motivo fosse suscetível de roubar fundos da empresa, os ataques também resultaram no vazamento de informações sobre saúde do paciente protegido (PHI) e/ou informações financeiras pessoais.[5]

Violações devido a roubo de credenciais não vão desaparecer. As organizações podem tentar proteger a si mesmas e seus funcionários e clientes através de treinamento de segurança, medidas de segurança de e-mail e autenticação mais forte. Mas até que o nome de usuário e a senha sejam substituídos por métodos mais seguros, o roubo de credenciais continuará a ser uma tática favorita para os invasores.

Este documento propõe que a ForgeRock Passwordless Authentication , baseada nos padrões da indústria, pode reduzir ou eliminar a confiança na autenticação baseada em nome de usuário e senha, e melhorar a postura de segurança da sua organização.

Mas primeiro, vejamos que alternativas estão em uso hoje.

Autenticação Forte

Muitas aplicações e serviços oferecem agora "autenticação forte", usando autenticação de dois fatores (2FA) ou autenticação multi fator (2FA exige que um usuário primeiro se autentique com um nome de usuário e senha e depois um segundo fator dependente de um código de acesso único (OTP). Estes são normalmente entregues através de um aplicativo autenticador, uma resposta a uma notificação push em um aplicativo móvel, ou com menos segurança sobre o protocolo de mensagens de texto SMS.

Com 2FA, o segundo fator de autenticação deve ser apresentado a cada tentativa de autenticação.

O MFA incorpora mais atributos contextuais mais tipos de autenticadores e mais contexto tais como dispositivo do utilizador, navegador, IP, localização ou hora do dia. Algumas soluções MFA podem exigir que o usuário autentique mais ou menos, dependendo do contexto da sessão.

> A mistura de dois ou mais tipos de fatores aumenta a segurança, mas a combinação de dois ou mais fatores não únicos pode fazer mais mal do que bem.

O princípio subjacente a estes dois métodos é que a autenticação forte deve exigir que o usuário se autentique com uma combinação de pelo menos dois fatores únicos. O nome de usuário e a senha são fatores de "conhecimento" (algo que eles sabem). O dispositivo móvel, token de hardware ou cartão inteligente são fatores de "posse" (algo que eles têm). E a biometria, como as impressões digitais ou os identificadores de reconhecimento facial, são exemplos de fatores de "herança" (algo que eles são).

Sites que exigem que os usuários se autentiquem através de um nome de usuário e senha e, em seguida, pedir ao usuário para apresentar outros fatores de conhecimento, tais como "questões de segurança" que o usuário pode esquecer ao longo do tempo, tornar inútil o segundo fator de autenticação. Respostas a perguntas de segurança comuns (exemplo: nome de solteira da mãe) estão disponíveis através de registros públicos, redes sociais, ou engenharia social.

2FA e MFA são mais seguros que a autenticação por nome de usuário e senha, mas eles também têm suas limitações. 2FA pode tornar se cansativo para os usuários que têm de autenticar sempre de duas maneiras, especialmente se envolver a mudança para uma aplicação autenticadora ou uma mensagem SMS para encontrar e depois introduzir o código de acesso único. O MFA pode ser difícil de implementar e muitas vezes depende da configuração de regras políticas que não proporcionam a agilidade e o granularizado minucioso que as equipes de segurança necessitam. Uma implementação bem sucedida de MFA ou 2FA também depende em grande parte da força e flexibilidade da identidade da organização e da solução de gerenciamento de acesso.

Uma Abordagem à Autenticação Baseada em Padrões

Uma autenticação forte é melhor servida por uma abordagem baseada em padrões que pode reduzir ou eliminar a dependência no nome de usuário e na senha. A empresa de análise Gartner recomenda a substituição de senhas por autenticação biométrica e prevê que 60% das empresas grandes e globais e 90% das médias empresas irão substituir as senhas por outros métodos para mais de 50% dos casos de uso de identidade até 2022.[6]

Navegador, sistema operacional e fornecedores de hardware estão assinando a aliança FIDO e estão oferecendo suporte ao FIDO2.[7]

Em 2019, o World Wide Web Consortium (W3C) ratificou o padrão Fast Identity Online 2 (FIDO2) Web Authentication (WebAuthn), que permite uma autenticação sem nome de usuário e sem uso de

O padrão original FIDO, também conhecido como Universal 2 Fator (U2F), usa um modelo de chave pública/privada escalável, onde um novo par de chaves é gerado para cada serviço, mantendo a separação entre pares de chaves para preservar a privacidade.[8] Ele permite autenticação "sem senha" para serviços online usando uma chave de segurança de hardware.

O novo padrão FIDO2 é a evolução "sem nome de usuário e sem senha" do FIDO, e depende de credenciais armazenadas localmente em um dispositivo do usuário. O FIDO2 consiste em duas especificações:

- Uma API baseada na web, chamada **Web Authentication (WebAuthn)**, permite autenticação "sem senha" para aplicações web usando criptografia de chave pública e autenticadores . A WebAuthn suporta credenciais baseadas no padrão original FIDO U2F e credenciais FIDO2.

- Um **Protocolo Cliente para Autenticador FIDO2 (CTAP2)**, permite a comunicação entre aplicações de clientes para autenticadores habilitados para FIDO2 por meio de navegadores e sistemas operacionais habilitados para FIDO2.

Tipos de autenticadores

O FIDO2 depende de pares de chaves públicas/privadas armazenadas com segurança em hardware local e navegadores compatíveis com o FIDO2 que interagem com os serviços para criar credenciais de chave pública/ privada segura para cada serviço. As chaves privadas em cada par de chaves são armazenadas localmente e nunca deixam o autenticador do usuário. As chaves públicas são usadas pelo servidor de autenticação para criptografar e assinar a comunicação com os dispositivos endpoint dos usuários.

A capacidade de armazenamento do autenticador local do usuário determina se podemos habilitar a autenticação "sem nome de usuário" e sem senha.

Os autenticadores de plataforma, baseados no trusted platform module (TPM) ou enclave seguro instalado em muitos laptops e telefones, são normalmente desbloqueados por um sensor biométrico, como no Microsoft Windows Hello ou Apple TouchID.

Os autenticadores de hardware "cross platform ", ou "roaming ", apresentam as reivindicações de acesso de um usuário a outro serviço ou dispositivo. Exemplos disso são as chaves de segurança do Google Titan, YubiKeys , ou autenticadores Duo que usam USB, comunicação near field (NFC), e Bluetooth. Quando ativado pela inserção em uma porta USB, pressionando um botão ou tocando, o autenticador envia uma resposta assinada que valida o login do usuário. Os Smartphones também podem funcionar como autenticadores.

Ao confiar nas credenciais seguras armazenadas no hardware confiável do próprio usuário, o FIDO2 WebAuthN permite a autenticação sem nomes de usuário e senhas, eliminando virtualmente o potencial de violação de dados relacionados ao roubo de credenciais.

ForgeRock Passwordless Authentication

ForgeRock Passwordless Authentication implementa o padrão FIDO2 WebAuthn no ForgeRock Intelligent Access. Ela permite que você projete jornadas de usuário seguras e perfeitas para autenticação sem senhas, e em casos, também sem nomes de usuário.

A ForgeRock Passwordless Authentication reduz a superfície de ataque da sua organização ao praticamente eliminar o roubo de credenciais resultante de ataques de phishing , reutilização de senha, preenchimento de credenciais, keyloggers e muito mais.

Benefícios da autenticação sem senhas

- **Seguro:** As credenciais de login são únicas para cada site, e nunca saem do dispositivo do usuário. Ao contrário do nome de usuário e da senha, as credenciais nunca são transmitidas no fio, eliminando assim os ataques de pessoa dentro do meio.
- **Conveniente:** Utiliza métodos integrados simples, tais como leitores de impressões digitais ou câmeras, ou utiliza chaves de segurança FIDO fáceis de utilizar. Os consumidores podem selecionar o aparelho que melhor se adapta às suas necessidades.
- **Privado:** As chaves são únicas e não podem ser usadas para rastrear os usuários através dos sites Os dados biométricos nunca deixam o dispositivo do usuário

“Estamos posicionados para dar a todos os nossos usuários uma experiência muito melhor através da eliminação de nomes de usuário e senhas, bem como reduzir as chamadas para a nossa central de atendimento para senhas esquecidas”.

— Doug Neumann, Gerente de TI, Estados Unidos, Administração Nacional de Segurança Nuclear

Como Funciona a Autenticação Sem Senha

A ForgeRock fornece autenticação sem senha através do ForgeRock Intelligent Access Trees e nós de registro e autenticação específicos da WebAuthn . Para utilizar a autenticação sem senha, o usuário deve primeiro se registrar autenticando com seu nome de usuário e senha no armazenamento de identidade, para que a ForgeRock possa identificar o usuário e o dispositivo.

Quando um usuário tenta registrar seu dispositivo pela primeira vez, o ForgeRock Intelligent Access detecta se o dispositivo suporta o padrão WebAuthn . Se o registro do dispositivo for bem sucedido, a ForgeRock instrui o dispositivo do utilizador a criar um único par de chaves públicas/privadas para comunicar com a ForgeRock . Quando o usuário autentica seu dispositivo usando o sensor biométrico embutido, a chave privada do usuário, que é armazenada com segurança na memória persistente e nunca deixa o dispositivo, fica disponível para assinar desafios de autenticação.

A ForgeRock emite um desafio ao dispositivo do usuário e criptografa o com a chave pública do usuário. A chave privada no dispositivo do usuário assina o desafio, que a ForgeRock verifica com a chave pública do usuário. Esse processo estabelece a conexão segura entre o dispositivo de hardware do usuário e a ForgeRock, para que eles possam usar autenticação
sem senha para logins subsequentes.

O nome de usuário tradicional e as jornadas de usuário baseadas em senha, emparelhadas com a autenticação adicional, devem ser mantidas como um método alternativo se o usuário não puder se autenticar com a ForgeRock usando seu dispositivo confiável registrado (exemplo: se o dispositivo confiável estiver indisponível, perdido ou roubado).

Usando autenticação sem senhas sem biometria

Algumas pessoas não podem usar a biometria, ou as suas organizações não a suportam. Pode ativar a autenticação sem senha com qualquer autenticador externo protegido por PIN (algo que conhece e que tem), como os cartões inteligentes ativados por FIDO2, FIDO2 ou chaves de segurança de hardware compatíveis com o Fator 2 universal (U2F), ou relógios inteligentes. A ForgeRock suporta os recursos sem senha de autenticação da Web FIDO2 para vários autenticadores, formatos e tipos de atestados. Para mais informações, leia o Solution Brief.

Configuração de Autenticação Sem Senha

Autenticação sem senha é um conjunto de recursos no ForgeRock Intelligent Access projetado para suportar o padrão FIDO2/ WebAuthn . Os usuários podem registrar dispositivos confiáveis e usar seu recurso incorporado para armazenar credenciais localmente. Existem três nós pré configurados em árvores de Intelligent Access. Esses nós podem ser simplesmente arrastados e soltos para a interface do usuário de Intelligent Access para criar jornadas de usuário. Para saber mais sobre árvores e nós de Intelligent Access, leia o documento técnico, “Introducing ForgeRock Intelligent Access.”

Registrando um dispositivo

Os usuários devem primeiro autenticar com seu nome de usuário e senha e, em seguida, registrar seu dispositivo antes que eles possam desfrutar de autenticação sem senha. Para habilitar isso, construa a jornada do usuário e adicione um Nó de Registro WebAuthn após a coleta de nome de usuário/senha e o nó de decisão do armazenamento de dados. Se o usuário registrar com sucesso um autenticador do tipo correto conforme determinado pelas propriedades do nó, a avaliação da árvore continua juntamente com o resultado de sucesso. A autenticação sem senha falhará se o cliente não tiver suporte ao WebAuthn por exemplo, se o navegador que eles estão usando não tiver suporte ou se ele se registrar com o tipo errado de autenticador. Um resultado de Erro do Cliente pode ocorrer quando o registro do cliente expira.

Validando a identidade do usuário

Qualquer autenticador usado para autenticação sem senha deve ser validado contra a identidade de um usuário para ser considerado seguro. As organizações devem validar os usuários para seus autenticadores pessoalmente ou usando um processo de prova de identidade digital confiável enquanto registram autenticadores. Para saber mais sobre os níveis de garantia de identidade e processos de comprovação de identidade digital que você pode construir no ForgeRock Intelligent Access, baixe o documento técnico, Reduce Government Services Fraud – Incorporate Identity Proofing Into Citizen Registration and Authentication.[9] Para saber mais sobre a incorporação de verificação de identidade baseada em crédito, leia o documento técnico, Reduce the Total Cost of Fraud.

Habilitando a autenticação sem um nome de usuário

Para tornar possível que o usuário se autentique sem inserir seu nome de usuário para autenticações futuras, alterne em “Nome de usuário para dispositivo” à direita do Nó de Registro.

Autenticar sem um nome de usuário requer que os autenticadores do usuário suportem o armazenamento de chaves de residente.

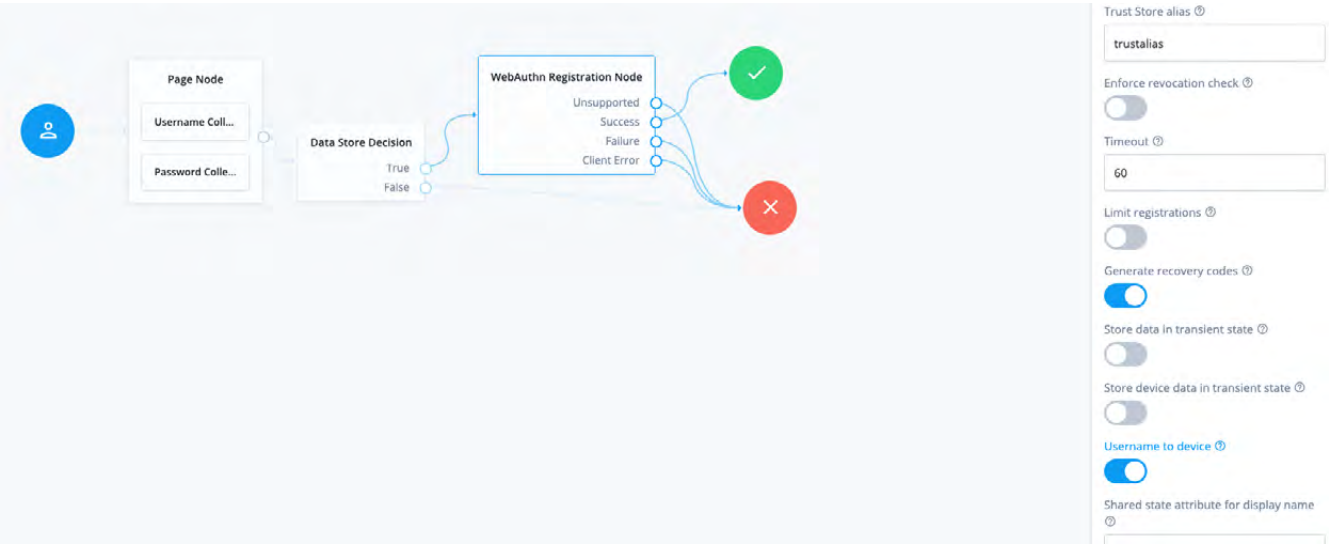

Figure 1: Registro sem senha com autenticação sem nome de usuário habilitada

Depois que o usuário se registra com sucesso e deseja fazer login o Nó de Autenticação WebAuthn executa e mostra ao usuário uma jornada de login “sem nome de usuário”

Analisando um dispositivo

Se você quiser realizar análises adicionais no dispositivo de um usuário e atrasar o registro de um dispositivo até que o resultado da análise esteja concluído, você pode adicionar o Nó de Armazenamento de Dispositivos WebAuthn na árvore de registro do WebAuthn . Este nó é opcional.

Aqui está um exemplo de como você pode usá-lo. Digamos que você queira ativar autenticação sem nome de usuário e sem senha, mas apenas para funcionários que estão usando laptops fornecidos pela
empresa feitos por um determinado fabricante e apenas para aqueles laptops instalados com um TPM biométrico. Você pode adicionar o Nó de Armazenamento do Dispositivo WebAuthn na árvore de registro, juntamente com um nó de decisão personalizado projetado para capturar dados de atestados específicos do dispositivo (exemplo: número de série e, para melhor segurança, uma cadeia de certificados para verificar se o dispositivo é genuíno). Isso impede que os usuários válidos se autentiquem de dispositivos não gerenciados e fortaleça a postura de segurança da sua organização.

Para habilitar o Nó de Armazenamento do dispositivo WebAuthn, alterne em “Armazenar dados em estado transitório” à direita da tela. O estado transitório significa que os dados do dispositivo são armazenados apenas em memória temporária, permitindo assim que a ForgeRock os use para análise.

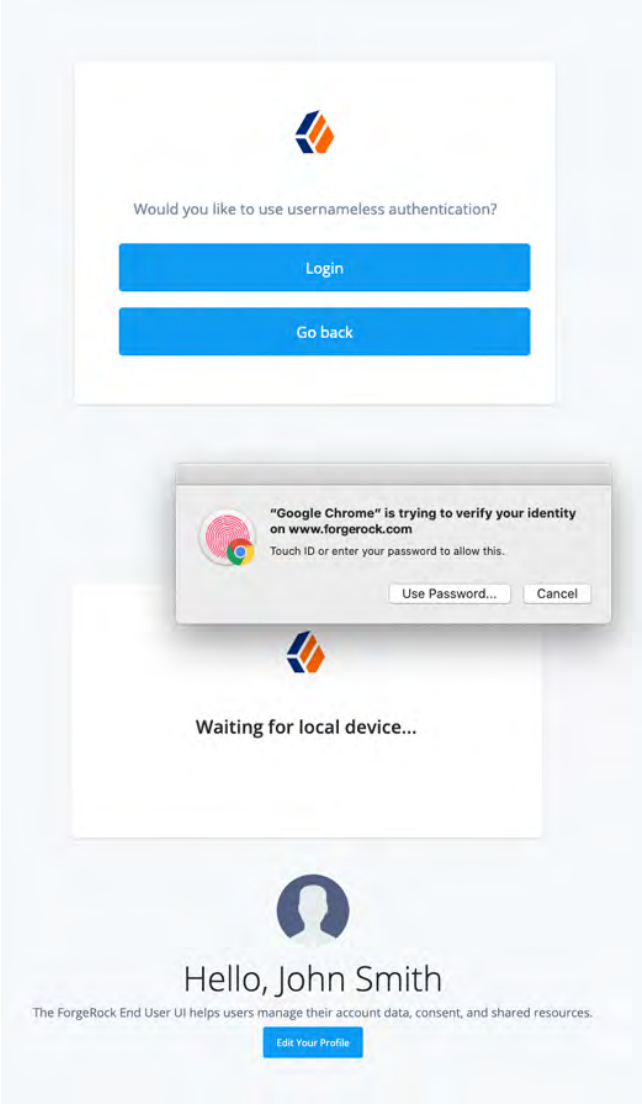

Figure 2: Autenticação sem nome de usuário

Figure 3: Nó de Armazenamento de Dispositivos WebAuthn em uma jornada de registro

Alternativas de autenticação sem senha

Os usuários devem sempre ter uma alternativa à autenticação sem senha se seu dispositivo registrado for perdido ou roubado ou se eles estiverem usando um navegador ou dispositivo que ainda não suporte as credenciais FIDO2 e WebAuthn . Você pode projetar jornadas de usuário que coletam credenciais de nome de usuário e senha e adicionar MFA, incorporando a plataforma Trusted Platform Module (TPM), push móvel ou autenticadores de terceiros.

Quando usar autenticação sem senha

A ForgeRock Passwordless Authentication é ideal para usuários da força de trabalho que autenticam em aplicativos na nuvem ou no local. A ForgeRock Passwordless Authentication pode ser usada tanto para autenticação inicial de login quanto para intensificação, incluindo autorização transacional. Para saber mais sobre autenticação intensificada e autorização transacional, leia o documento técnico, "**Introducing ForgeRock Intelligent Access**."

À medida que mais navegadores e aplicativos voltados para o consumidor começarem a suportar o FIDO2 e o padrão WebAuthn , você poderá projetar jornadas de usuário sem senha para casos de uso do cliente também. O padrão WebAuthn está sendo usado hoje em aplicativos de mídia social, serviços financeiros, jogos e armazenamento em nuvem.

A ForgeRock Passwordless Authentication pode ser usada tanto para autenticação inicial de login quanto para intensificação, incluindo autorização transacional.

Conclusão

O ForgeRock Intelligent Access facilita o design de autenticação segura rapidamente sem nomes de usuário e senhas para casos de uso da força de trabalho e do consumidor. Você pode projetar essas jornadas do usuário em minutos e suportar vários autenticadores simultaneamente, permitindo uma economia significativa de custos em relação a soluções de autenticação fortes e legadas. A ForgeRock Passwordless Authentication oferece melhor segurança, conveniência e privacidade para seus usuários

[1] https://fidoalliance.org/what-is-fido/
[2] https://www.welivesecurity.com/2020/03/19/security-flaws-found-in-popular-password-managers/
[3] https://enterprise.verizon.com/resources/reports/dbir/
[4] https://www.forgerock.com/resources/2020-consumer-identity-breach-report
[5] https://www.unitypoint.org/filesimages/About/Security%20Substitute%20Notification.pdf
[6] https://www.gartner.com/smarterwithgartner/embrace-a-passwordless-approach-to-improve-security/
[7] https://www.theverge.com/2020/6/24/21301509/apple-safari-14-browser-face-touch-id-logins-webauthn-fido2
[8] https://www.yubico.com/blog/what-is-fido2/
[9] https://www.forgerock.com/resources/whitepaper/reduce-government-services-fraud