O maravilhoso mundo sem senhas (com abordagem ZeroTrust + Passwordless)

“Hackers don’t break in, they log in!”, Bret Arsenault, CISO na Microsoft.

Atualmente é muito comum, ao acessarmos um site ou sistema, deparar-se com a solicitação de autenticação para que o usuário possa ser identificado e ter seu acesso concedido.

Houve uma evolução muito grande nos últimos anos no processo de autenticação com a utilização de identidade híbrida, reduzindo assim a necessidade de que os usuários criassem diversas contas, porém, um ponto ainda permaneceu nos sistemas: o método de autenticação mais utilizado ainda é feito por meio de senhas.

Esse método de autenticação, apesar de muito tradicional, seja por sua simplicidade ou por costume dos usuários, possui diversas desvantagens, como:

- Os usuários evitam a utilização de senhas aleatórias, o que apesar de aumentar a segurança dificulta a sua memorização para posterior utilização.

- Usuários tendem a sempre utilizar senhas mais simples contendo informações pessoais, o que facilita um ataque de força bruta baseado em dicionário.

- Senhas podem serem guardas em locais de fácil acesso ou capturadas por programas durante sua utilização permitindo que posteriormente sejam utilizadas para acessos indevidos.

Além do mais, sempre visando aumentar a segurança no processo de autenticação, muitas vezes são adicionadas mais camadas de autenticação reduzindo a praticidade e permanecendo o problema na base.

Outra estratégia utilizada, visando aumentar um pouco mais a segurança, é a solicitação de troca de senha frequente, o que cria um cenário propício ao surgimento de senhas sequenciais ou que possuem um padrão simples de ser descoberto.

Assim temos o desafio de tornar o processo de autenticação mais seguro e, ao mesmo tempo, mais prático.

A resposta para esse desafio seria um pouco contraintuitiva, mas a ideia é retirar o elo fraco da corrente, ou seja, “retirar a senha” / Passwordless, conforme já havia previsto Bill Gates, em 2004, na RSA Conference.

Utilizando um quadrante cujo eixo horizontal é a praticidades e o vertical a segurança temos o seguinte resultado:

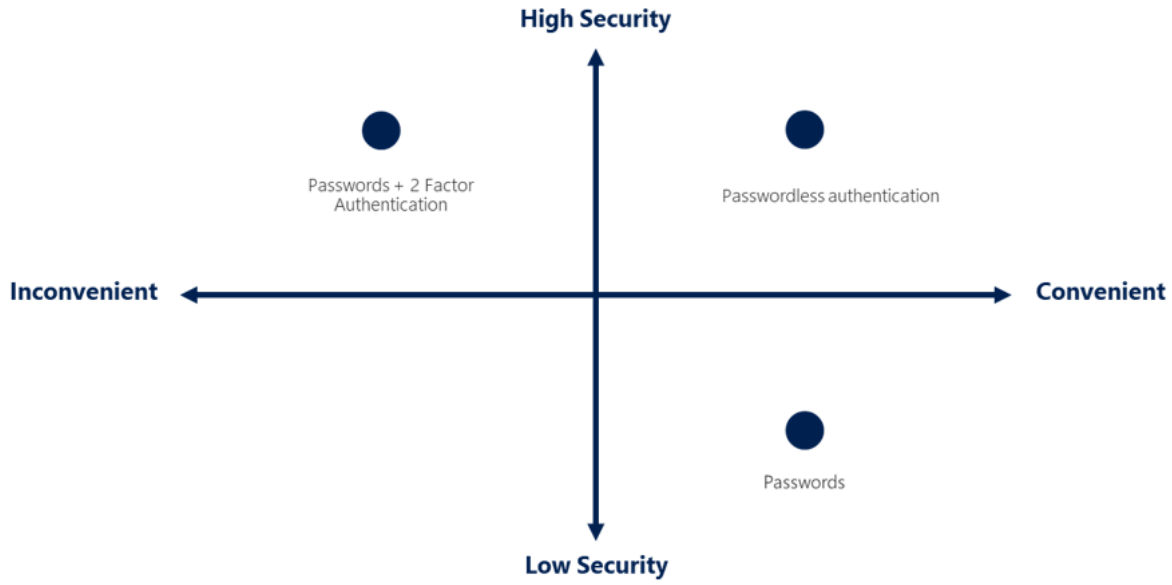
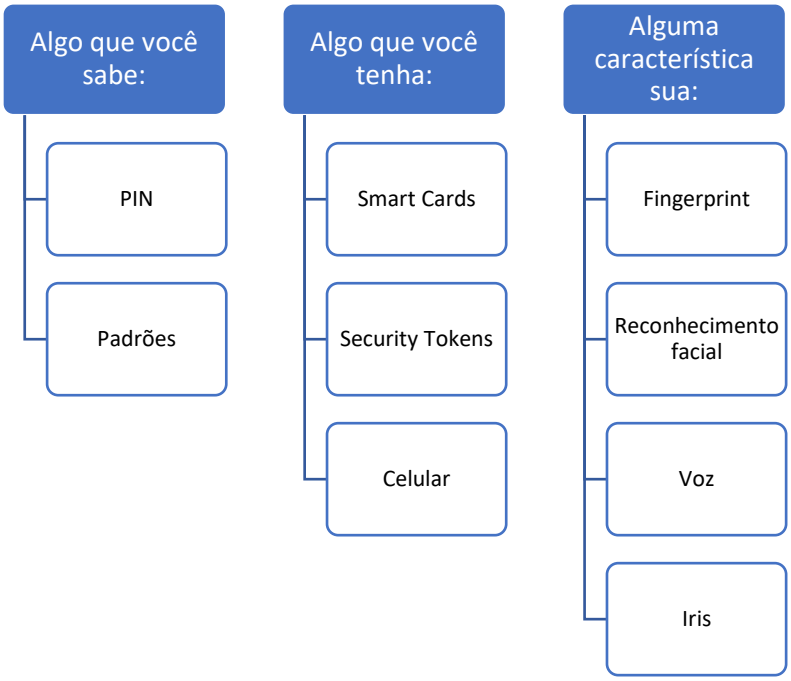


Figura 1 - Segurança x Praticidade na autenticação

Mas o que seria Passwordless?

Passwordless é um meio de autenticação no qual o usuário não precisaria mais digitar sua senha para se autenticar, pois seria utilizado um ou mais dos três pilares abaixo:



Essa tecnologia já vem sendo anunciada, implementa e utilizada por alguns anos, conforme podemos ver no artigo A breakthrough year for passwordless technology - Microsoft Security Blog.

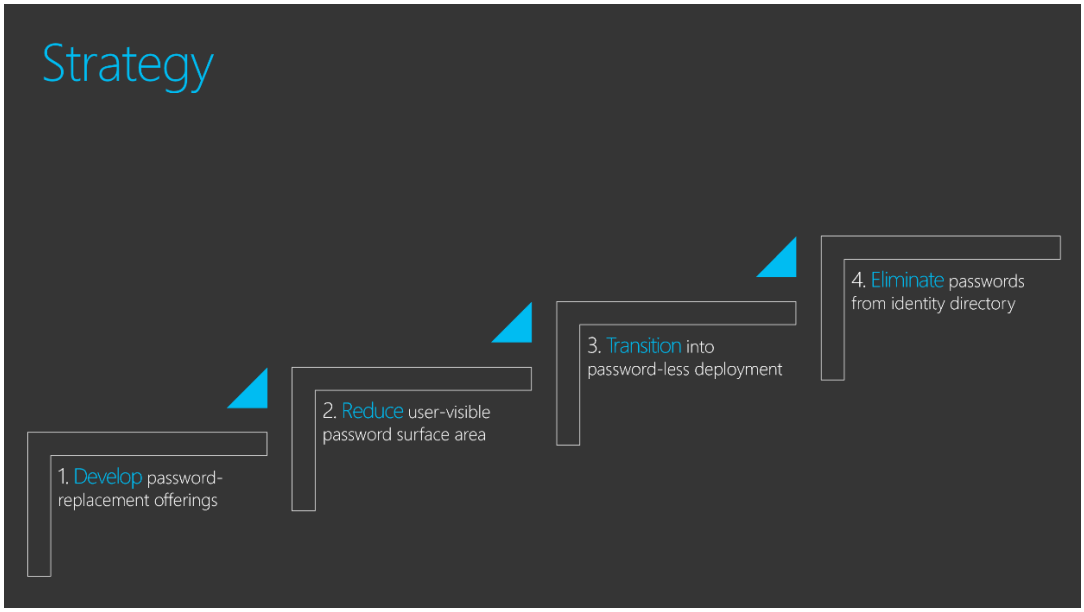
Essa funcionalidade foi disponibilizada para todas as organizações que utilizam o Azure AD em março de 2021 (Passwordless authentication is now generally available! - Microsoft Tech Community) e em setembro do mesmo ano para todos os usuários que possuem Microsoft Account (How to go passwordless with your Microsoft Account).

PasswordLess + Zero-Trust

A utilização de passwordless em uma abordagem Zero-Trust vem de maneira a simplificar, reduzir o custo de implantação e garantir maior eficiência, pois será exigido um menor número de ferramentas para evitar um vazamento, captura e reutilização das senhas.

Com o passwordless, o usuário terá mais agilidade nos seus acessos tornando a experiência algo muito melhor do que ter que se autenticar utilizando senha e depois ainda utilizar um novo fator de autenticação.

Para a jornada de migração para o PasswordLess no Windows é definido 4 passos a serem seguidos (Password-less strategy - Windows security | Microsoft Docs):



Primeiramente será inserido um método de autenticação que não precisa do uso de senhas, por exemplo, Windows Hello for Business.

No segundo passo, o foco será a redução do uso da senha para que o usuário comece a achar estranho locais onde são solicitadas a sua senha.

A terceira etapa consistirá em três sub etapas, nas quais:

- O usuário não precisa digitar sua senha.
- O usuário não precisa mais alterar sua senha.
- O usuário irá esquecer sua senha.

Atingindo a última sub etapa poderemos eliminar as senhas da base de diretório garantindo um ambiente sem senhas.

REFERÊNCIAS

1. Azure Active Directory passwordless sign-in - Microsoft Entra | Microsoft Docs
2. Passwords: If We're So Smart, Why Are We Still Using Them? - Microsoft Research
3. The passwordless future is here for your Microsoft account - Microsoft Security Blog