

CyberSecurity

Bret Mills

To Cross the Bridge of Death You Must Answer These Questions Three!



1

DISCLAIMER

- **This presentation is for information only.**
Evaluate risks before acting based on ideas from this presentation.
- **This presentation contains the opinions of the presenters.**
Opinions may not reflect the opinions of Tandem.
- **This presentation is proprietary.**
Unauthorized release of this information is prohibited.
Original material is copyright © 2024 Tandem.



2



Bret Mills


Security+, CISA, CISSP
Audit and Security Consultant



3

Agenda

- 1** Current Password Standards and Password Managers
- 2** Multi-Factor Authentication (MFA)
- 3** Passwordless Authentication



4

Is this a good password?

Spring2024!123



5

Is this a good
password?

Spring2024!123

@y%75T+r4YLnVQww



6

Current Password Guidance

1**NIST**

The minimum password length that should be required depends to a large extent on the threat model being addressed.

2**CIS**

14-char password-only, 8-char password+MFA, complex, annual change

3**CoNetrix**

14-character, complex, 90-day change



7

So, what is the answer?



8

Password Managers



9

Password Managers

PROS

1. Don't have to remember multiple passwords.
2. Can generate more complex passwords.
3. Can use Security Features (MFA).

CONS

1. When you can't remember your main password.
2. Not helpful if you choose easy-to-guess passwords.
3. Passwords are stored on someone else's server.



10

Multi-Factor Authentication



11

Multi-Factor Authentication (MFA)

PROS

1. More difficult to hack.
2. Convenient for user.
3. Easy to update with new safeguards.
4. Heavily embedded in M365.

CONS

1. Can be expensive to implement.
2. Can be difficult for users to accept (I don't want it on my phone, and I am not going to carry around that USB!).
3. MFA fatigue.



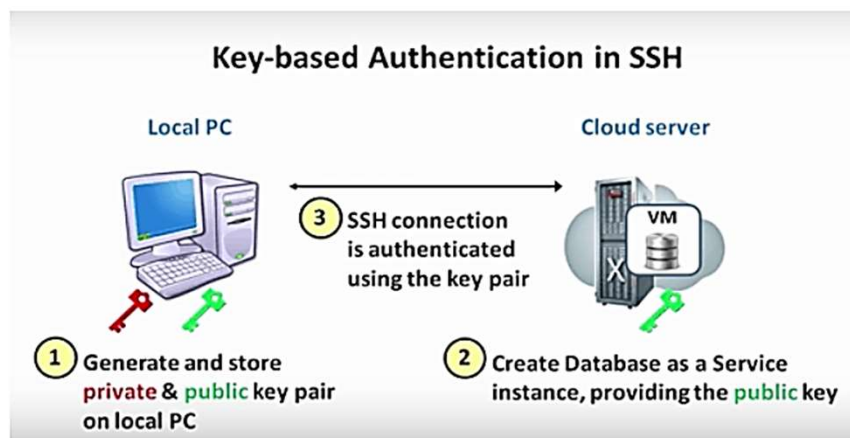
12

Passwordless

Trying to create a world where users **never type** their password, **never change** their password, and **do not know** their password.



13



From K21 Academy



14



15

Passwordless

PROS

1. Don't have to remember passwords.
2. The security of key exchange.

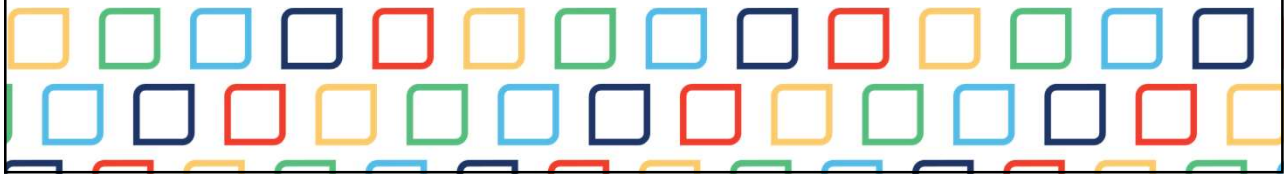
CONS

1. Not easy to setup.
2. Compatibility issues.

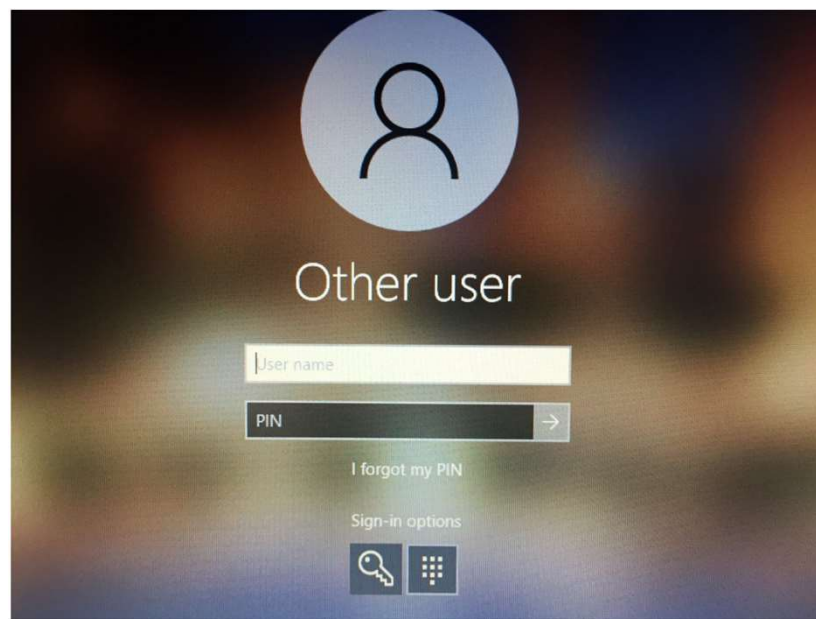


16

Well, Hello, Windows Hello for Business!



17



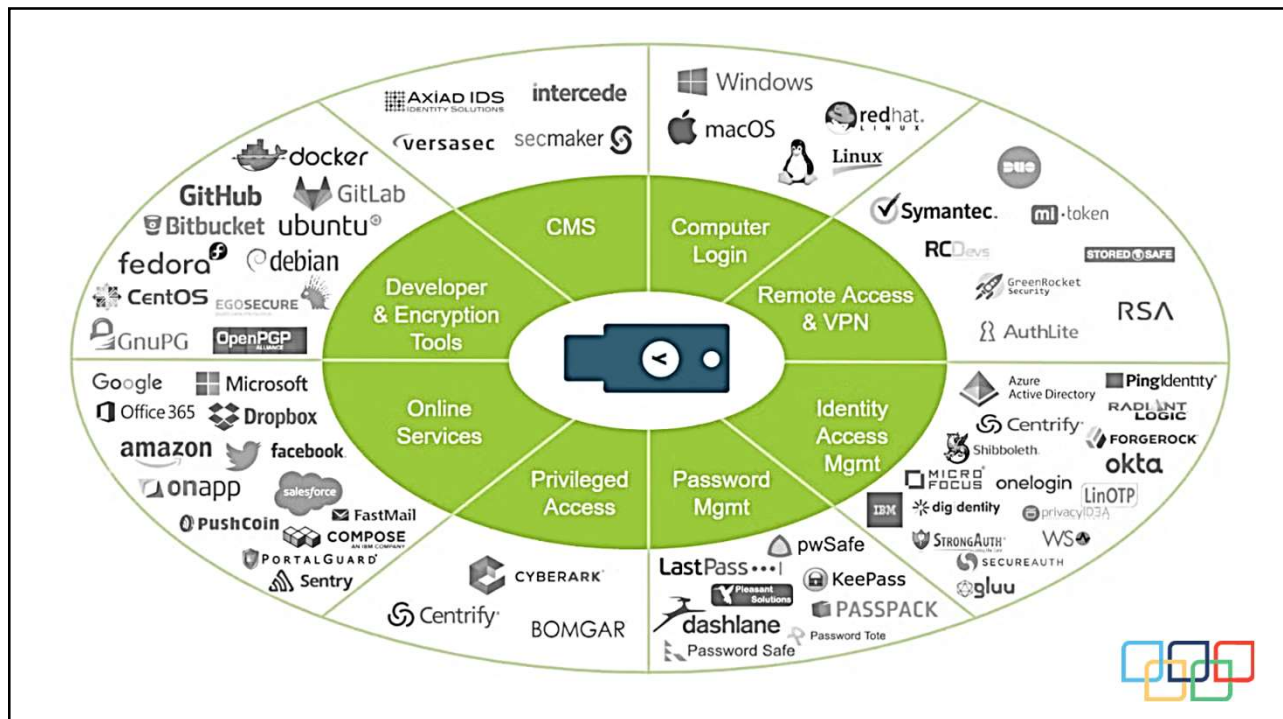
18

Passwordless Authentication

1. An Authenticator
2. FIDO2 (Fast Identity Online) Keys or Devices (YubiKey).



19



20

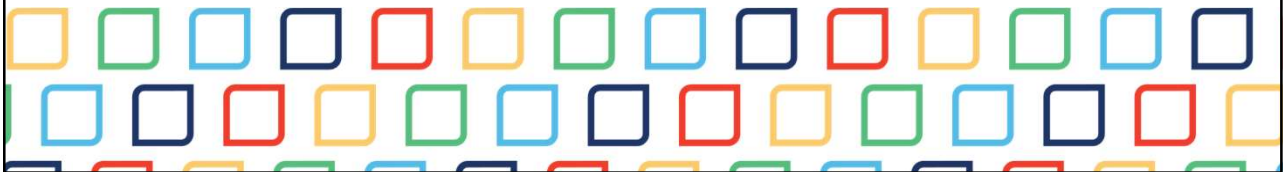
Passwordless Authentication

1. An Authenticator
2. FIDO2 (Fast Identity Online) Keys or Devices (YubiKey).
3. Certificate Based.
4. Cloud Kerberos Trust and AD Federation servers.



21

**So, what is best for
MY organization?**



22

What Now?

1 Risk assess!!!

Keep up to date with new technology.

2

3 Get help if you don't understand.

Stay away from
the Gorge of Eternal Peril!!!

4



23

Questions?

24