Azure Meetup
TORINO

welol
beyond the digital

#GlobalAzureTorino

RETELIT

TD SYNNEX

Azure Meetup
TORINO

#GlobalAzureTorino

(Password)less is more

Pietro Visentin
Riccardo Corna

#GLOBALAZURE 2023

RETELIT TD SYNNEX welol beyond the digital

WhoAmI

...o meglio... WhoAreWe

Pietro Visentin

Head of Security

Moresi.com

Riccardo Corna

MVP Security

Microsys

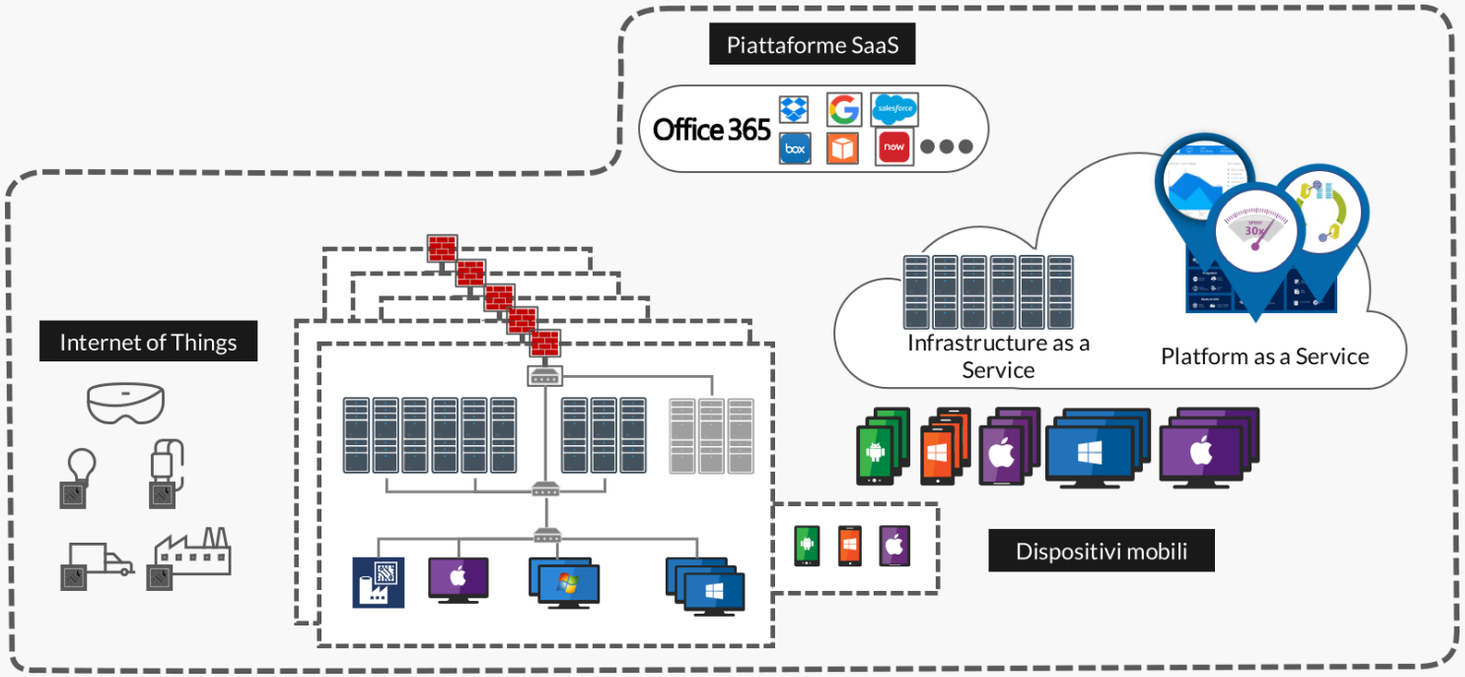
Agenda

Whoami
La posizione centrale dell’identità
Key takeaways 2022
Attacchi alle password
Perchè la MFA non basta più?
Come proteggerci meglio?
Metodi di autenticazione passwordless
DEMO

La posizione centrale dell'identità

Il ruolo centrale dell’identità

Per quanto la protezione infrastrutturale e dei device rimane fondamentale, l’identità assume sempre più un ruolo centrale.



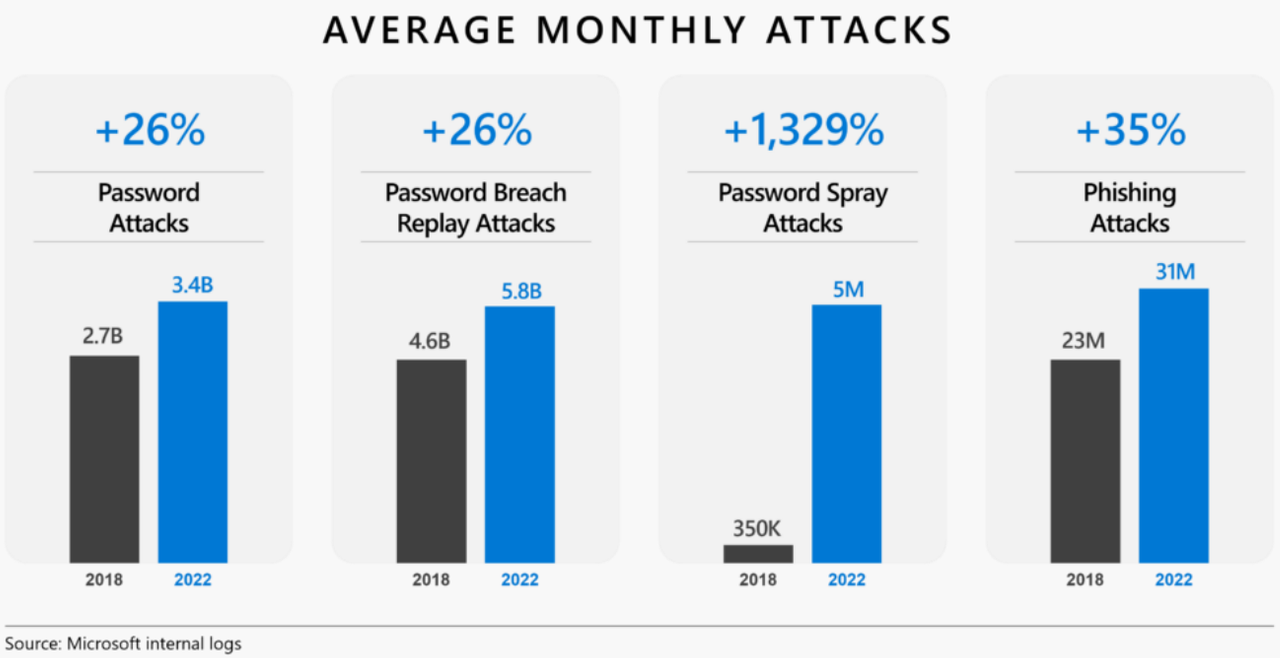
Identità e Security

Gli attacchi a infrastrutture e device sono preceduti da una compromissione dell'identità.

L’identità è il nuovo perimetro da proteggere.

Key Takeaways 2022

Attacchi alle password - 1



- Microsoft respinge più di 1.000 attacchi relativi alle password al secondo.
- Più del 90% degli account compromessi non hanno l'autenticazione multifattoriale abilitata.

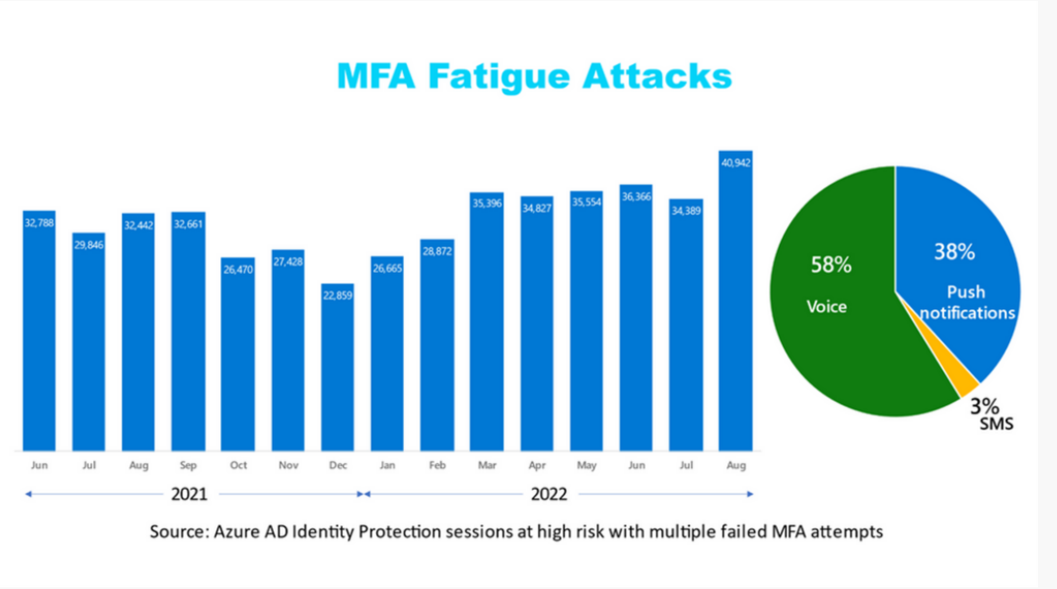
Attacchi alle password - 2

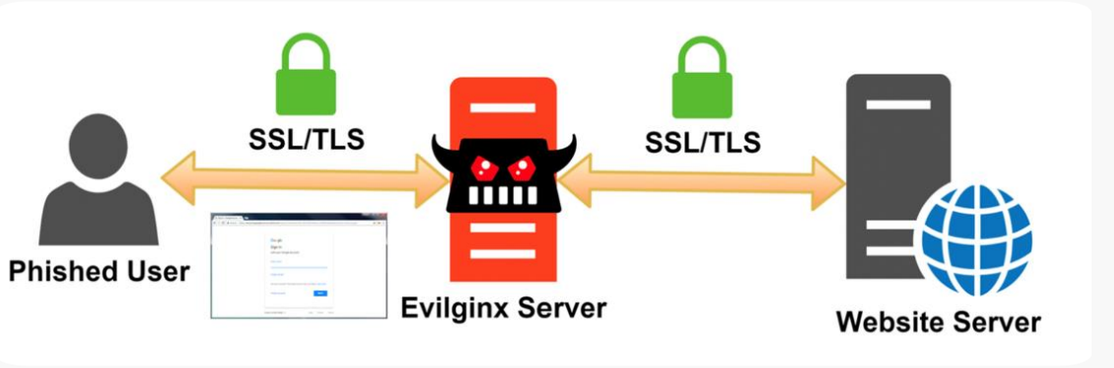
Password spray	Provare ad utilizzare password comuni su più account.
Phishing	Convincere qualcuno a digitare le proprie credenziali su un sito web falso o in risposta a un testo o a un'e-mail.
Breach replay	Basarsi sul riutilizzo pervasivo delle password per prendere le password compromesse su un sito e provarle con altri.

Perchè la MFA non basta più?

Attacchi alla MFA - 1

SIM-jacking	Vulnerabilità della telefonia
Hammering o griefing	Un push ripetuto del secondo fattore di autenticazione, fino a che l'utente approva per sfinimento
Adversary-in-the-middle	Ingannano gli utenti per farli interagire con l'autenticazione a più fattori.





Attacchi alla MFA – 2 - Riflessioni

Il 29% degli utenti su Microsoft 365 e Azure il mese scorso ha effettuato un login multifattoriale.

Molti tenant hanno ancora i legacy protocol abilitati

L'utilizzo dell'autenticazione a più fattori è la cosa più importante che possiamo fare.

Come proteggerci meglio?

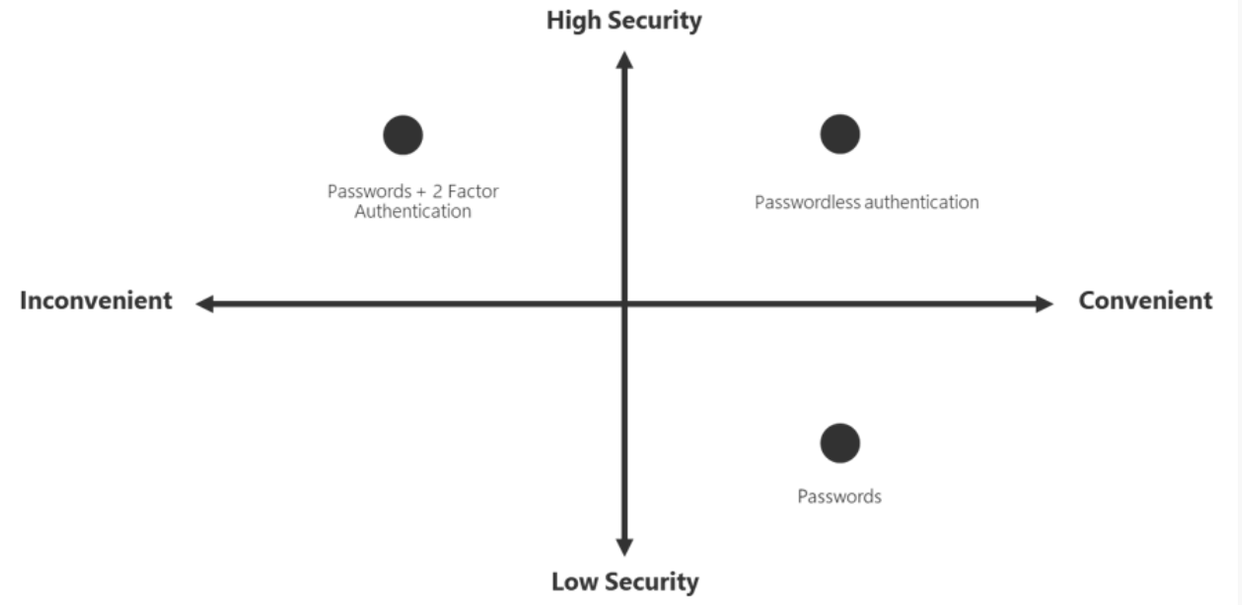
L'autenticazione passwordless è un metodo di autenticazione che elimina l'uso delle password e le sostituisce con altri fattori di autenticazione come biometrici o di possesso

Risorse

- *How to configure passwordless in Azure AD connected environments*

Passwordless is more!

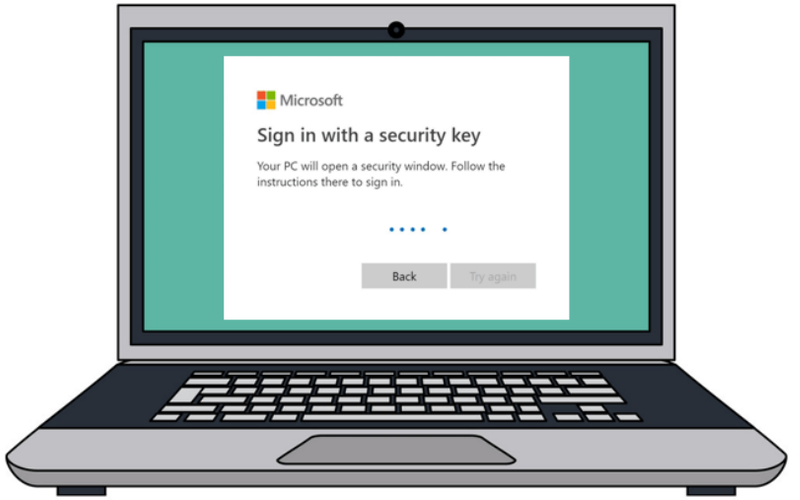
- Authenticator
- Windows Hello for Business
- FIDO2
- Certificate Based Authentication

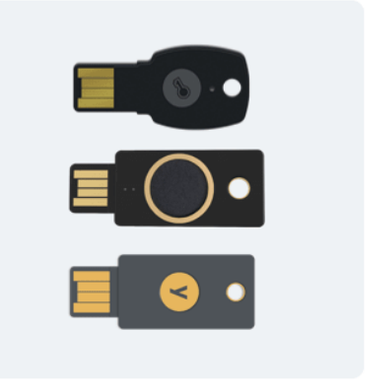


Metodi di autenticazione passwordless

FIDO2 Key

- Hardware: nessun username o password esposti
- Phishing resistant
- Incorpora WebAuthn
- NON supportato su mobile



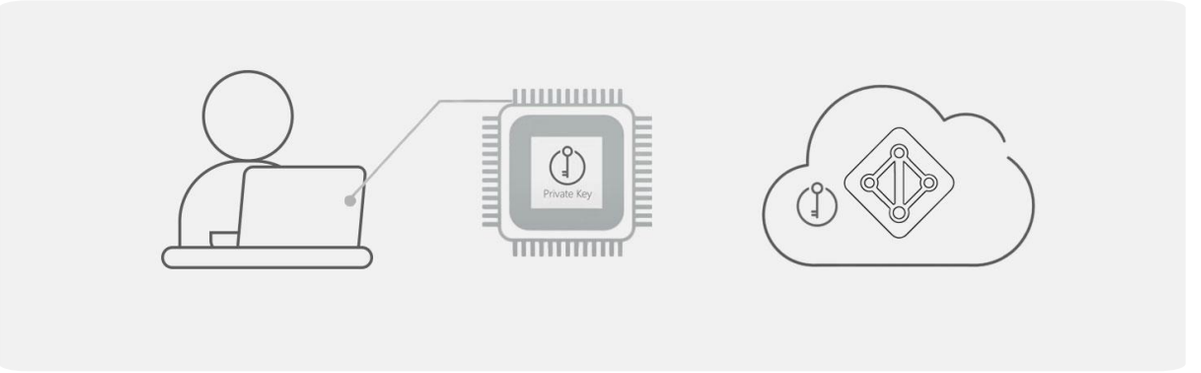


Risorse

- *Passwordless con FIDO2*

Windows Hello for Business

- Perché il PIN non è una password
- «MFA» al login
- Almeno il TPM come requisito
- Naturale complemento di SSPR
- Access to on prem resources

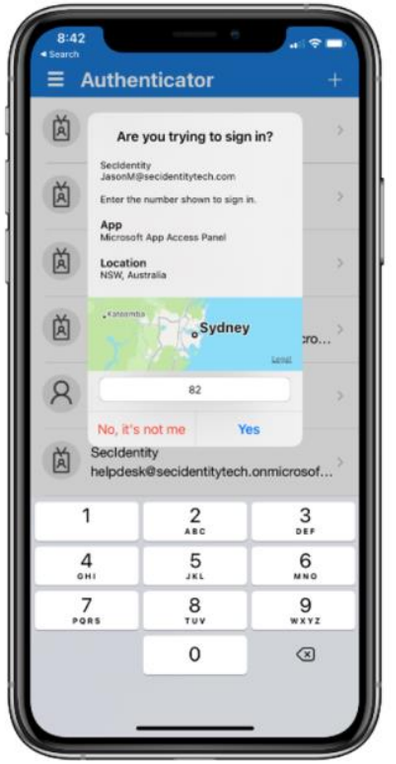


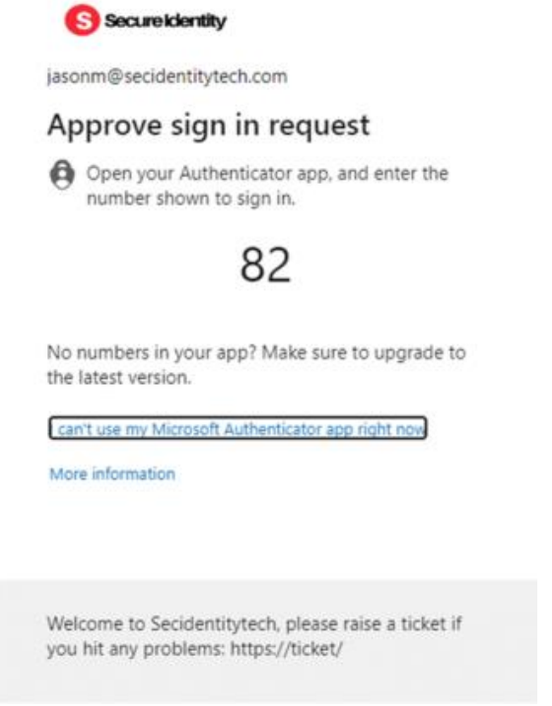
Risorse

- *WhFB è una MFA!*

Authenticator

- Sempre avere l'ultima versione di Authenticator app
- Supportati più tenant [iOS]... ma il dispositivo deve essere registrato in ogni tenant
- In lavorazione multiple accounts su Android
- NON supportati gli account guest
- Per iOS, consigliato abilitare **Microsoft Authenticator** -> **Settings** -> **Usage Data**



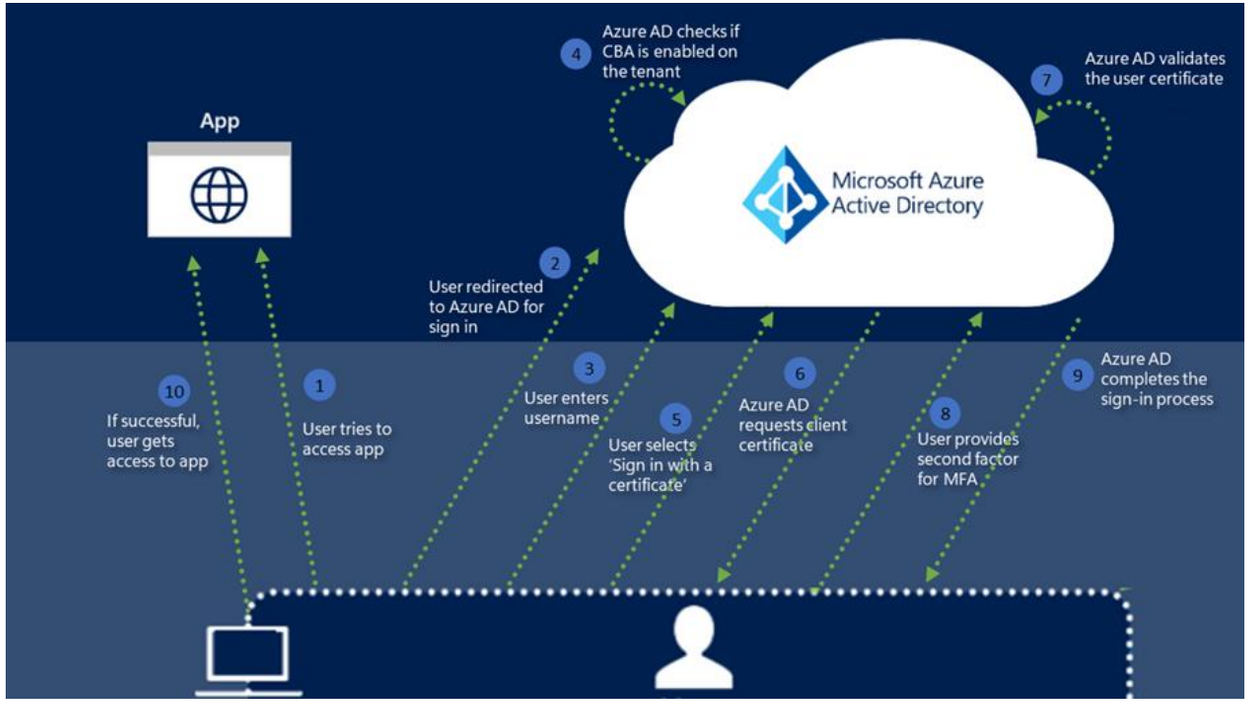


Risorse

- *Passwordless con Authenticator*

Certificate Based Authentication [AAD]

- Elimina la necessità di ADFS
- Semplificazione regole networking
- Riduce la dipendenza da infrastrutture on-prem
- Può essere usata come fattore aggiuntivo [single-factor CBA] oppure Multi-Factor
- Facile mappatura da portale degli attributi certificato-utenza
- Disponibile da **Azure AD Free** in su
- Compatibile con Authentication Strength



Risorse

- *Sono autenticato... Ho il certificato!*

Authentication Methods Definitive Map

Method	PHR	Passwordless	SSPR	Winlogon	RDP (AD)	RDP (AAD)	RADIUS	Mobile	Web	Primary Factor	2nd Factor
Password Only	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✗
FIDO2 Security Key	✓	✓	✗	✓	◐	✓	✗	✗	✓	✓	✓
Microsoft Authenticator (Push)	✗	✗	✓	✗	✗	✓	✓	✓	✓	✗	✓
Microsoft Authenticator (Passwordless)	✗	✓	✗	✗	✗	✓	✗	✓	✓	✓	✗
Windows Hello for Business	✓	✓	✗	✓	◐	✓	✗	✗	✓	✓	✗
Certificate on a Smart Card	✓	✓	✗	✓	✓	✓	✓	◐	✓	✓	✓
Software TOTP Token	✗	✗	✓	✗	✗	✓	✓	✓	✓	✗	✓
Hardware OATH Token	✗	✗	✓	✗	✗	✓	✓	✓	✓	✗	✓
SMS	✗	✗	✓	✗	✗	✓	✓	✓	✓	✓	✓
Temporary Access Pass	✗	✗	✗	✓	◐	✓	✗	✓	✓	✓	✗
Voice Call	✗	✗	✓	✗	✗	✓	✓	✓	✓	✗	✓
Email OTP	✗	✗	✓	✗	✗	✓	✗	✓	✓	✓	✗
Security Questions	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗

DEMO

#GlobalAzureTorino

Volete quotidianamente contenuti come questi?

Siete appassionati di security e di tecnologie Microsoft?

SEGUITECI!

Microsoft Security Italian Users Group

ITSpecialist.cloud

Azvise.com


BY COMMUNITY • FOR COMMUNITY •
#GLOBALAZURE
2023
TORINO