

**— WEBINAR: DIE ZUKUNFT IST PASSWORTLOS:  
MAXIMALE SICHERHEIT UND KOMFORT MIT  
WINDOWS HELLO & PASSKEYS**

 first frame  
networkers



# HERZLICH WILLKOMMEN



**PHILIPPE HIRZEL**

**Projektleiter Security Services  
first frame networkers ag**

**Vielen Dank, dass Sie sich die Zeit für uns  
nehmen!**

**Webinar: Die Zukunft ist passwortlos:  
Maximale Sicherheit und Komfort mit Windows  
Hello & Passkeys**

**Das Webinar wird in Schweizerdeutsch gehalten.**

## UNSER REFERENT



**DANILO GIACOMINI**

**Senior System Engineer &  
Projektleiter  
first frame networkers ag**

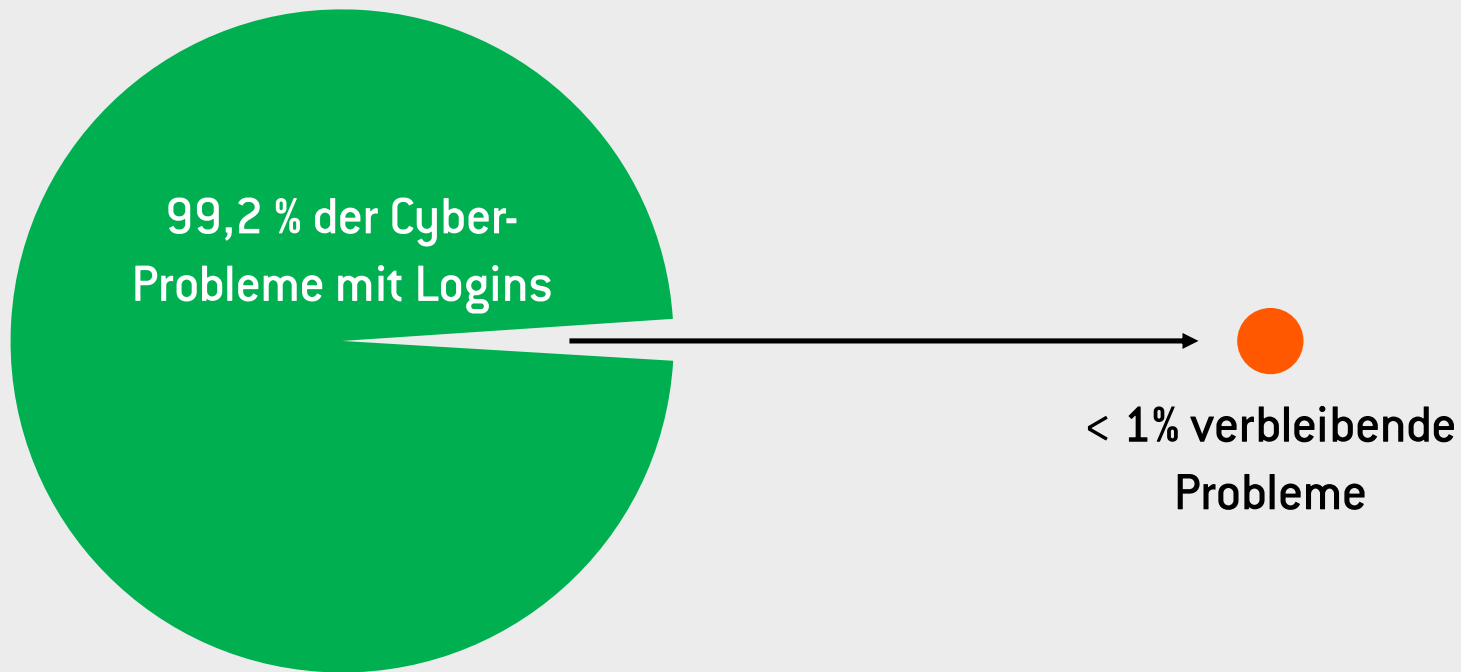
- ↔ Seit 2 Jahren bei der first frame networkers ag.
- ↔ Aufgabe: Projektleiter und System Engineer
- ↔ Ausbildung: eidg. dipl. Wirtschaftsinformatiker
- ↔ In seiner Freizeit genießt er seine Familie und schraubt am Homelab Zuhause.

# AGENDA

- ⇒ 11:00 Begrüssung / Philippe Hirzel
- ⇒ 11:05 Warum klassische MFA nicht mehr reicht / Philippe Hirzel
- ⇒ 11:15 Phishing-Resistant Authentication: Optionen, Strategie und Rollout / Danilo Giacomini
- ⇒ 11:25 Aus der Praxis: So begleiten wir unsere Kunden bei der Umsetzung / Danilo Giacomini
- ⇒ 11:35 Fragen & Antworten
- ⇒ 11:45 Schluss

**Fragen können mit der Chatfunktion gestellt werden.**

# MFA IST ESSENZIELL



Microsoft Digital Defense Report 2024

# FAKTOREN FÜR AUTHENTIFIZIERUNG



- Etwas das man **weiss**
- Z.B. ein Passwort
- Kann verraten werden

- LinkedIn Passwörter wurden gestohlen
- Mark Zuckerberg hatte das Passwort «**dadada**»
- Auch auf Twitter & Pinterest



- Etwas das man **hat**
- Z.B. ein Smartphone
- Kann gestohlen werden



- Etwas das man **ist**
- Z.B. ein Fingerabdruck
- Kann gefälscht werden

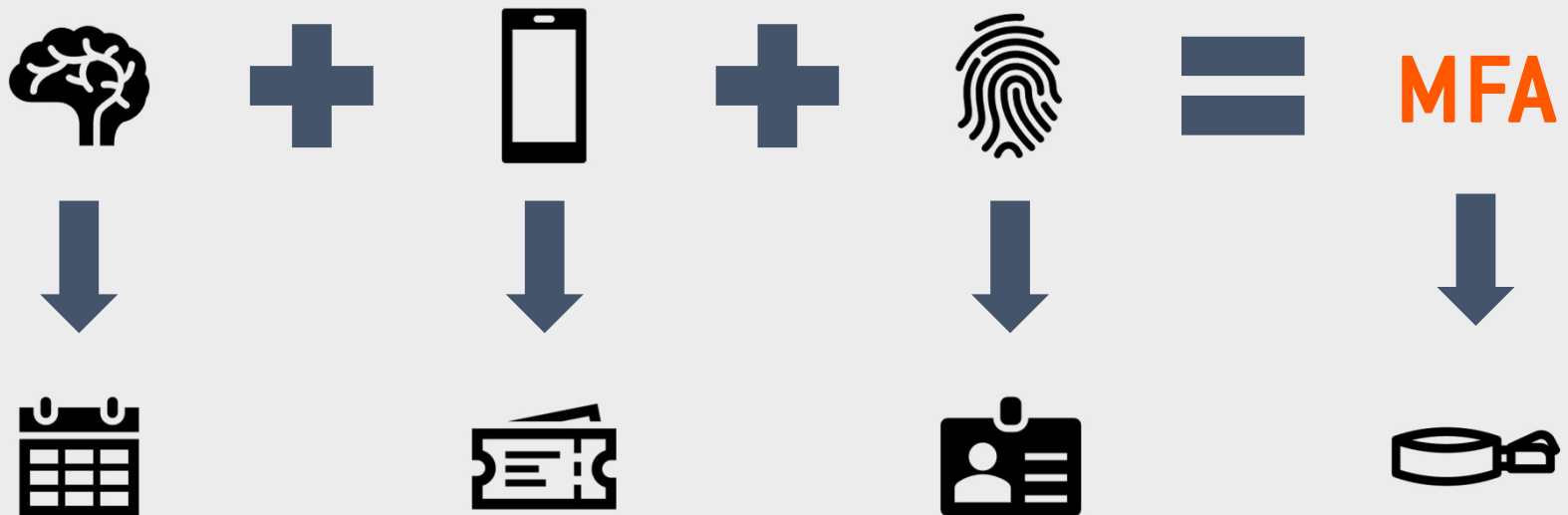
# MFA – MULTI FAKTOR AUTHENTIFIZIERUNG



# WIESO KANN EIN ACCOUNT ÜBERNOMMEN WERDEN?

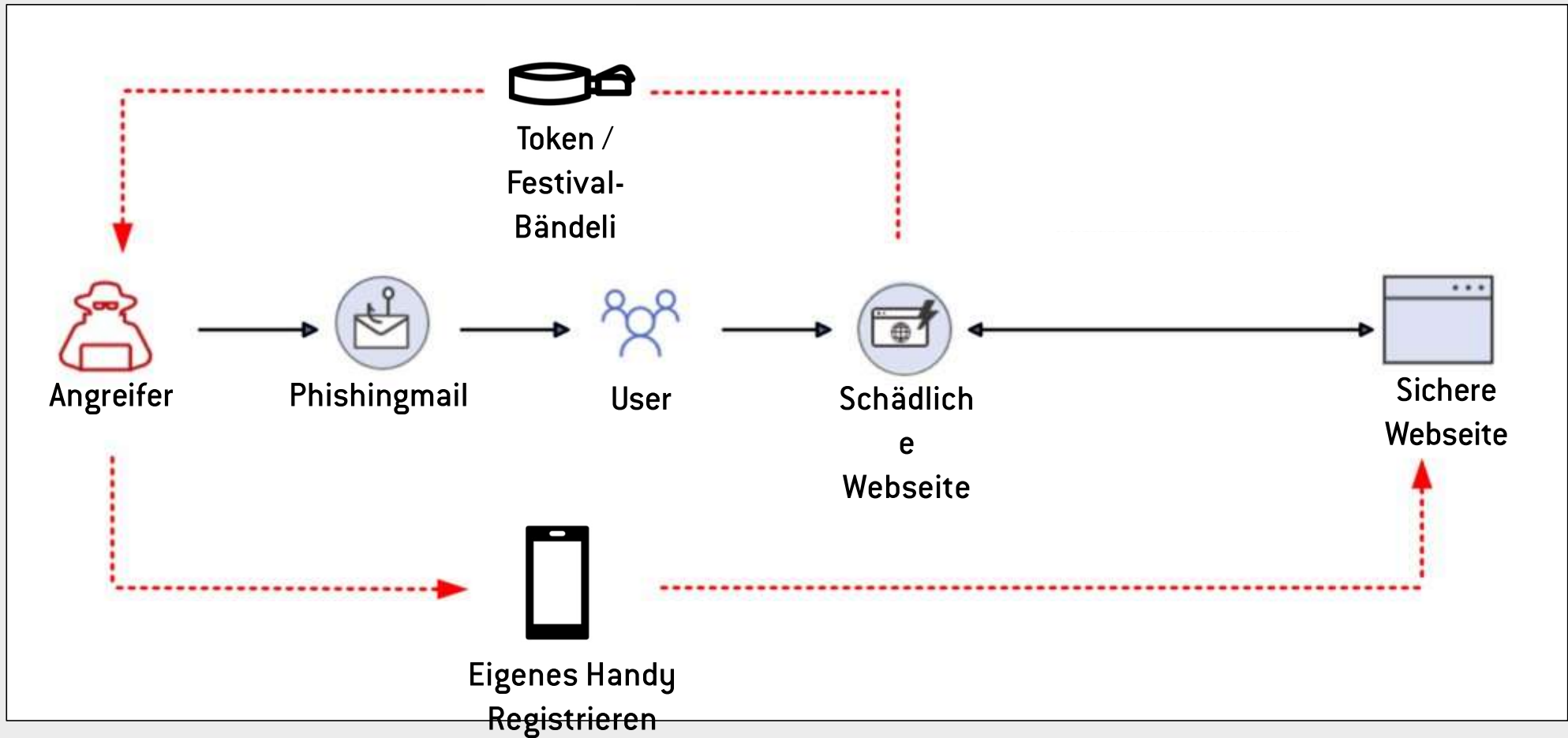


# WIESO KANN EIN ACCOUNT ÜBERNOMMEN WERDEN?



# WIESO KANN EIN ACCOUNT ÜBERNOMMEN WERDEN?

first frame networkers





## Sign in

Email, phone, or Skype

[No account? Create one!](#)

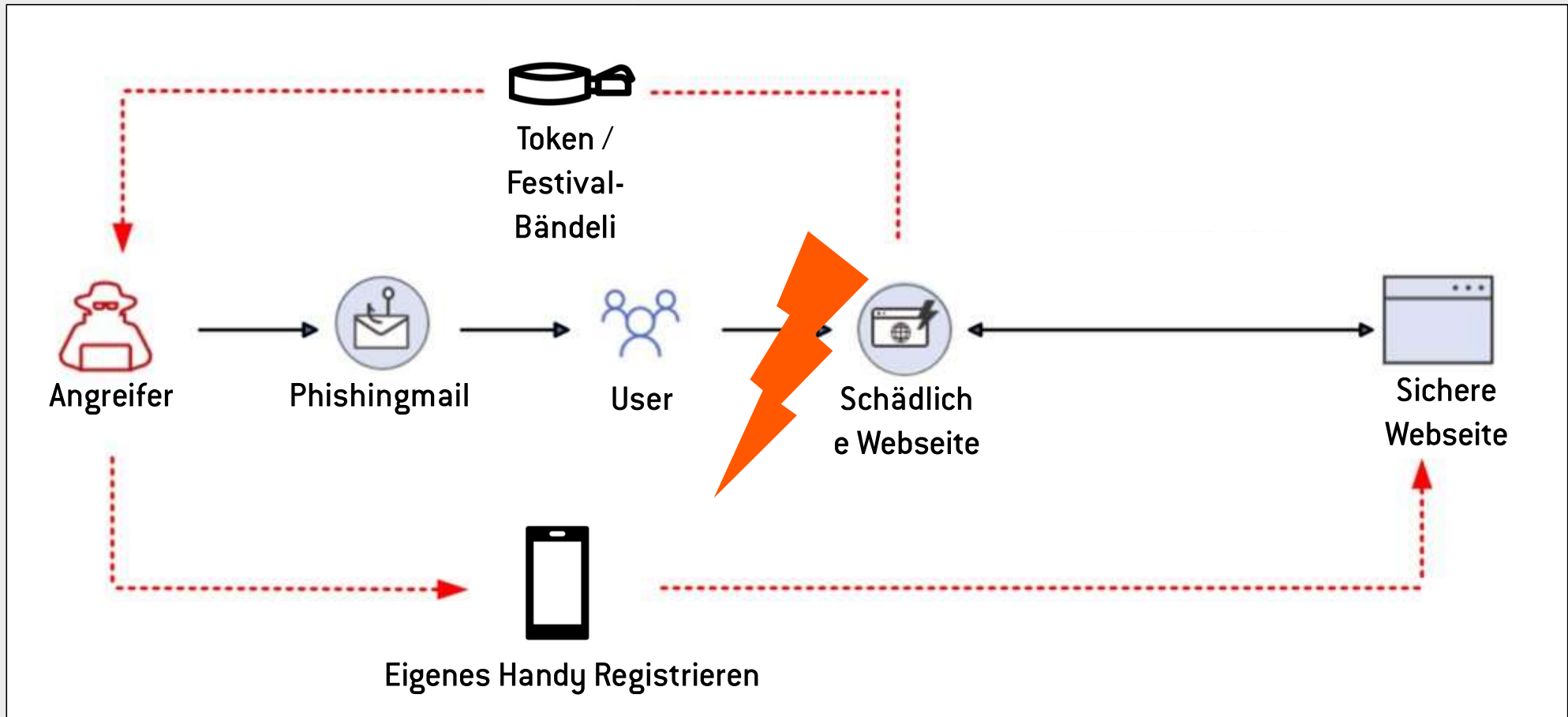
[Can't access your account?](#)

Next

 [Sign-in options](#)

# WIESO KANN EIN ACCOUNT ÜBERNOMMEN WERDEN?

first frame networkers



# WIESO REICHT MFA NICHT MEHR

79%

Account übernommen trotz MFA

1'265%

Zunahme von Phishing-Emails seit Launch von ChatGPT

0

Erfolgreiche Phishing-Angriffe bei Cloudflare seit FIDO-Rollout

81%

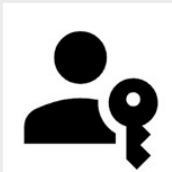
weniger Login-Helpdesk-Tickets nach Passkey-Rollout gemäss FIDO Alliance

Quellen: [FRSecure Incident Report 2025](#) · [SlashNext State of Phishing 2023](#) · [Cloudflare Post-Mortem Blog 2022](#) · [FIDO Alliance Passkey Index 2025](#)

# PHISHING RESISTANT AUTH

Bedeutet:

- Device Bound oder Domain Bound
- Braucht Asym. Crypto.



- Passkey
- Gute Idee, Praktikabilität noch zu verbessern



- Hardware Security Token
- Am sichersten jedoch etwas umständlich



- Windows Hello for Business
- Optimal für User auf Business Devices

# — WAS IST ÜBERHAUPT EIN PASSKEY?



## Passwort

– EdkgR35\*>5fç



## Passphrase

– Webinar-Passkey-Sicher!



## Passkey



# PASSKEY

## Device Bound



- Passkey ist an Hardware gebunden
- Anmeldung nur auf einem Gerät möglich
- Hardware
  - Smartphone
  - Yubikey
- Was passiert wenn ich mein Smartphone verliere?

## Synced



- Passkey kann zwischen Geräten synchronisiert werden
- Aktuell nur innerhalb Ökosystem wie iOS / Android / Microsoft
- Wohin werden Passkeys überall synchronisiert?



Neue Technologie welche sich noch bewähren muss – Ideal für technisch interessierte

# PASSKEY

## Vorteile



- Zum Anmelden sehr Benutzerfreundlich
- Kann nicht auf fake Website eingegeben werden
- Sicherlich besser als immer das Gleiche Passwort

## Nachteil



- Wo habe ich überall einen Passkey?
- Sync zwischen Geräten umständlich
- Geht auf Mobile nicht immer (Kombi: OS + Browser + Site)



Passkey für private Verwendung auf einem Gerät ideal (Handy)

## FIDO KEY

- ↔ Login an Hardware gebunden (Crypto-Chip auf FIDO Key)
- ↔ Physischer Stick wie z.B. Yubikey
- ↔ Geht auf Smartphones nicht immer



Ideal für alle Administratoren

# WINDOWS HELLO FOR BUSINESS



# — WINDOWS HELLO FOR BUSINESS

- ↔ An Hardware gebunden (TPM)
- ↔ PIN
- ↔ Fingerabdruck
- ↔ Gesichtserkennung
- ↔ Notebook mit IR-Kamera

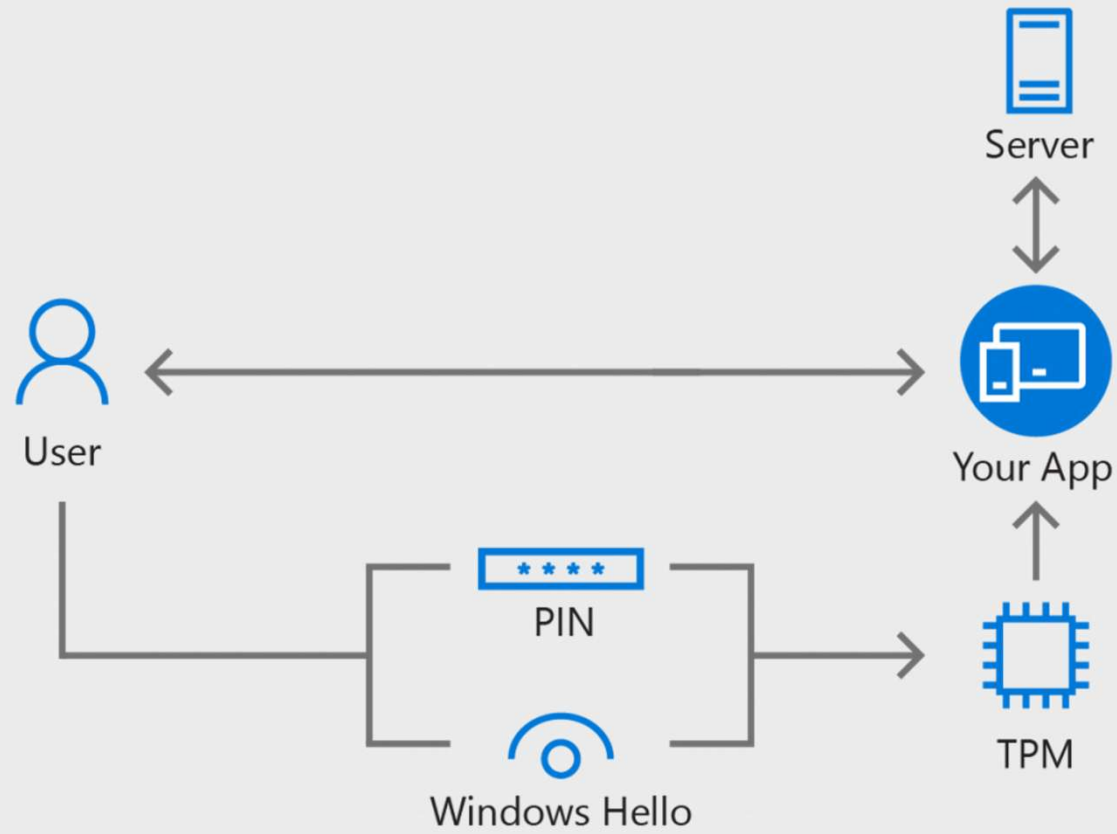


Ideal für alle Benutzer

# ONBOARDING WINDOWS HELLO FOR BUSINESS

1. IT-Team und Early Adopters zuerst
2. Benutzer Mitnehmen
3. Conditional Access ebenfalls beachten
4. Breakglass Accounts implementieren
5. Legacy Apps identifizieren

# ANMELDUNG



# — LIVE DEMO



# AUSBLICK

Generative KI hat die Spielregeln etwas verändert.



## NEXT STEPS

### ↻ Let's Talk!

↻ Mit Ihrem Account Manager

↻ Mit Philippe Hirzel [philippe.hirzel@firstframe.net](mailto:philippe.hirzel@firstframe.net) oder +41 41 768 08 60

↻ Mit Danilo Giacomini: [danilo.giacomini@firstframe.net](mailto:danilo.giacomini@firstframe.net) oder +41 41 768 08 00

### ↻ Weitere Infos

↻ [Detaillierte Information Security Operations Center](#)

↻ [Verschiedene Blog-Artikel zum Thema IT-Security](#)

## FEEDBACK-FORMULAR



- ↪ Herzlichen Dank für Ihre Teilnahme am heutigen Webinar.
- ↪ Ihre Meinung ist uns sehr wichtig.
- ↪ Daher bitten wir Sie um eine Minute Ihrer wertvollen Zeit für die Feedbackumfrage.
- ↪ Unter allen ausgefüllten Fragebögen verlosen wir einen **Bontique-Gutschein** im Wert von CHF 75.—.
- ↪ Den Link finden Sie auch im Chat:  
<https://forms.cloud.microsoft/e/UtAbWSRxGP>

Herzlichen  
Dank