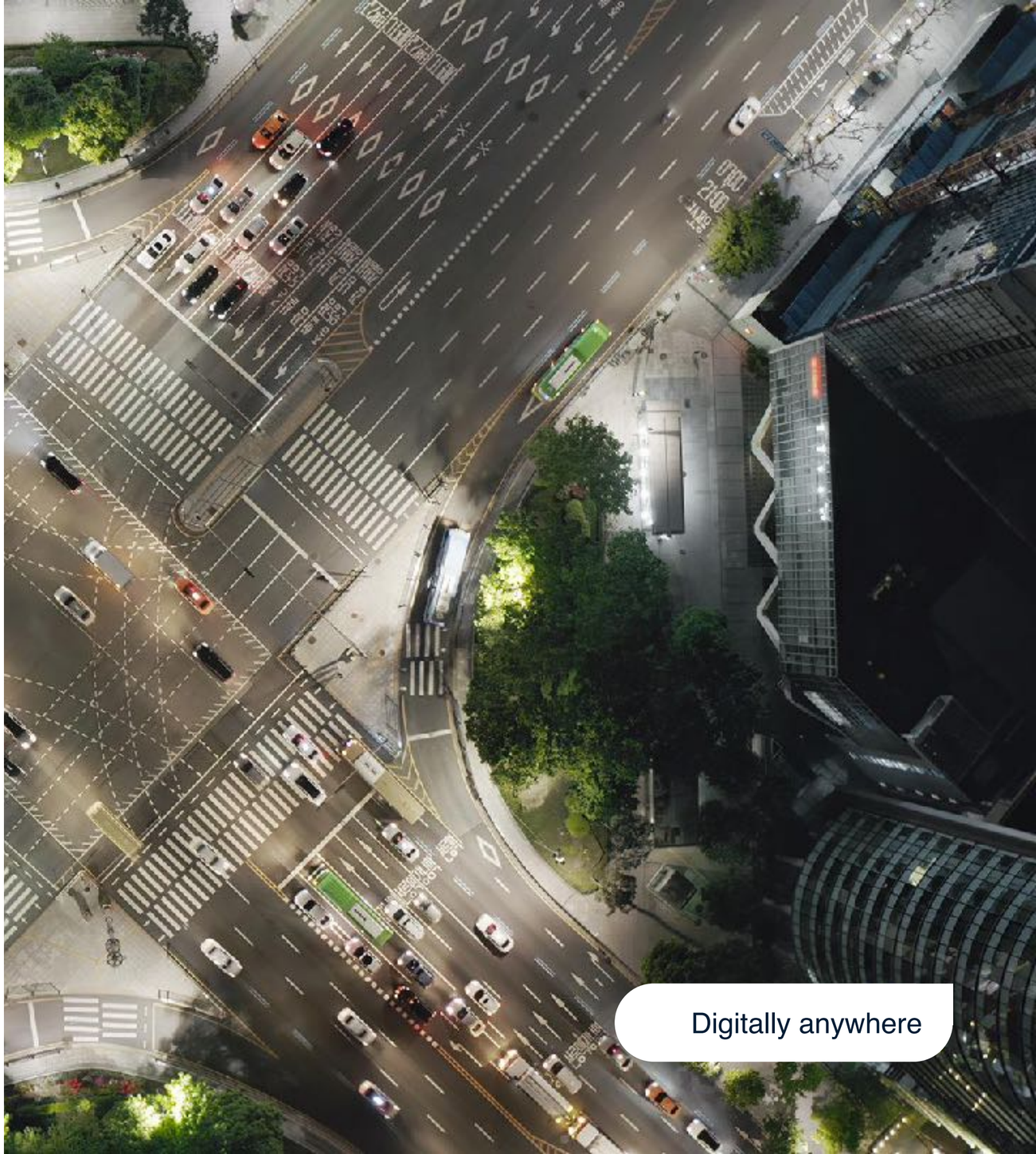
ProID

Bezpečná digitální identita a autentizace

Ondřej Mareček
Sales Manager, ProID

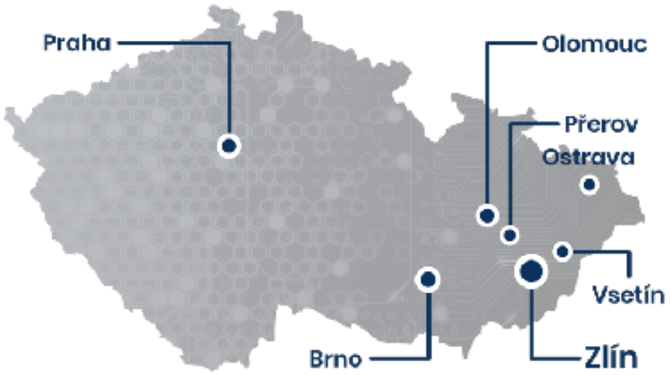


MONET+ v číslech

25+
let zkušeností

440+
zákazníků

350
zaměstnanců



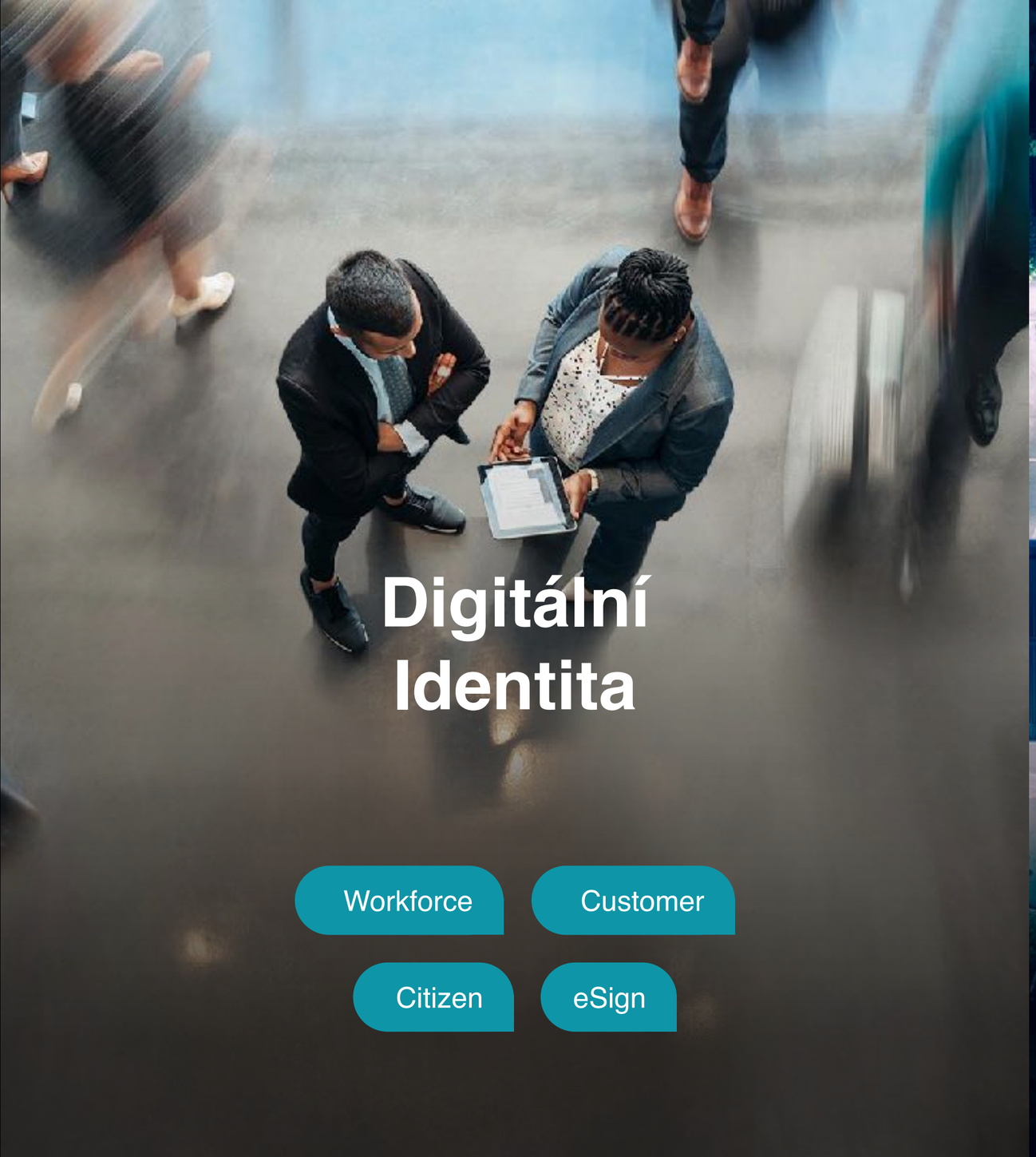
1 MISE

Tvoříme důvěryhodný digitální svět

8
business solutions

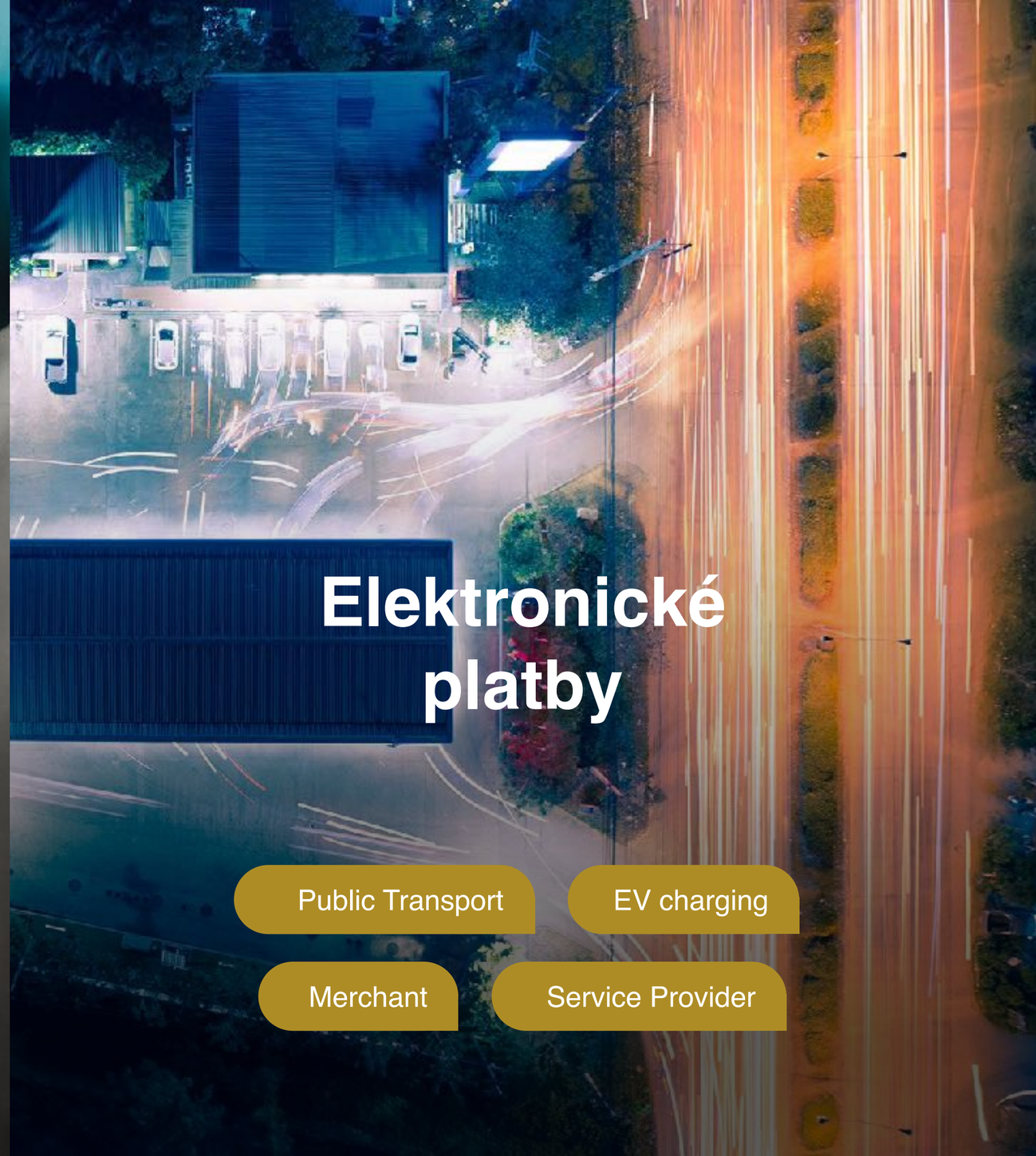
26,5M €
obrat za rok 2024

20+
zemí s rozpracovanými projekty



Digitální Identita

- Workforce
- Customer
- Citizen
- eSign



Elektronické platby

- Public Transport
- EV charging
- Merchant
- Service Provider

Povinná osoba - nZoKB

NIŽŠÍ REŽIM

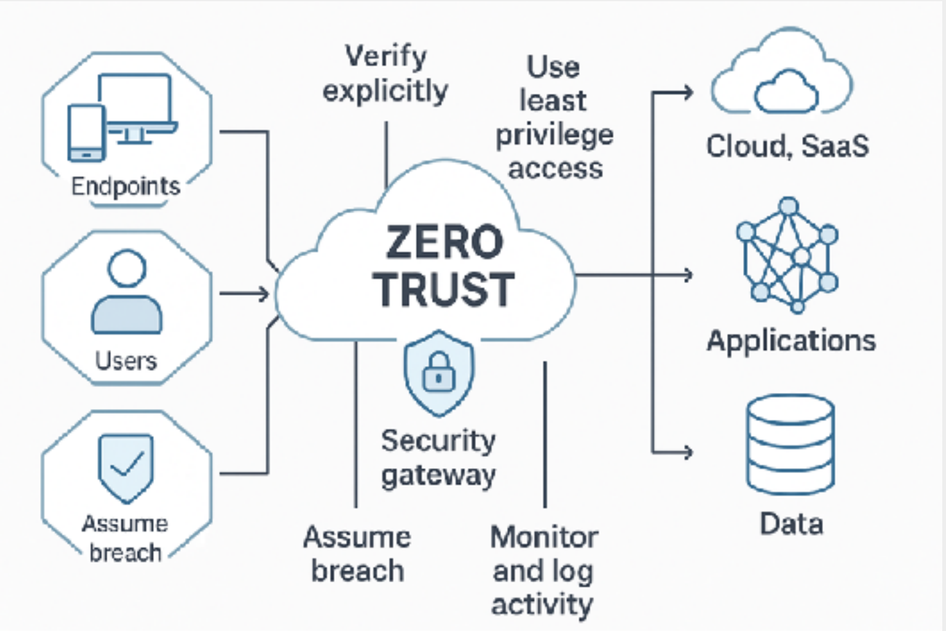
- Přiděluje minimální oprávnění nezbytně nutná pro výkon práce
- **Více-faktorovou autentizaci** nebo
  - autentizaci založenou **na modelu nulové důvěry**
- Přechodně hesla (12/17/22 znaků)

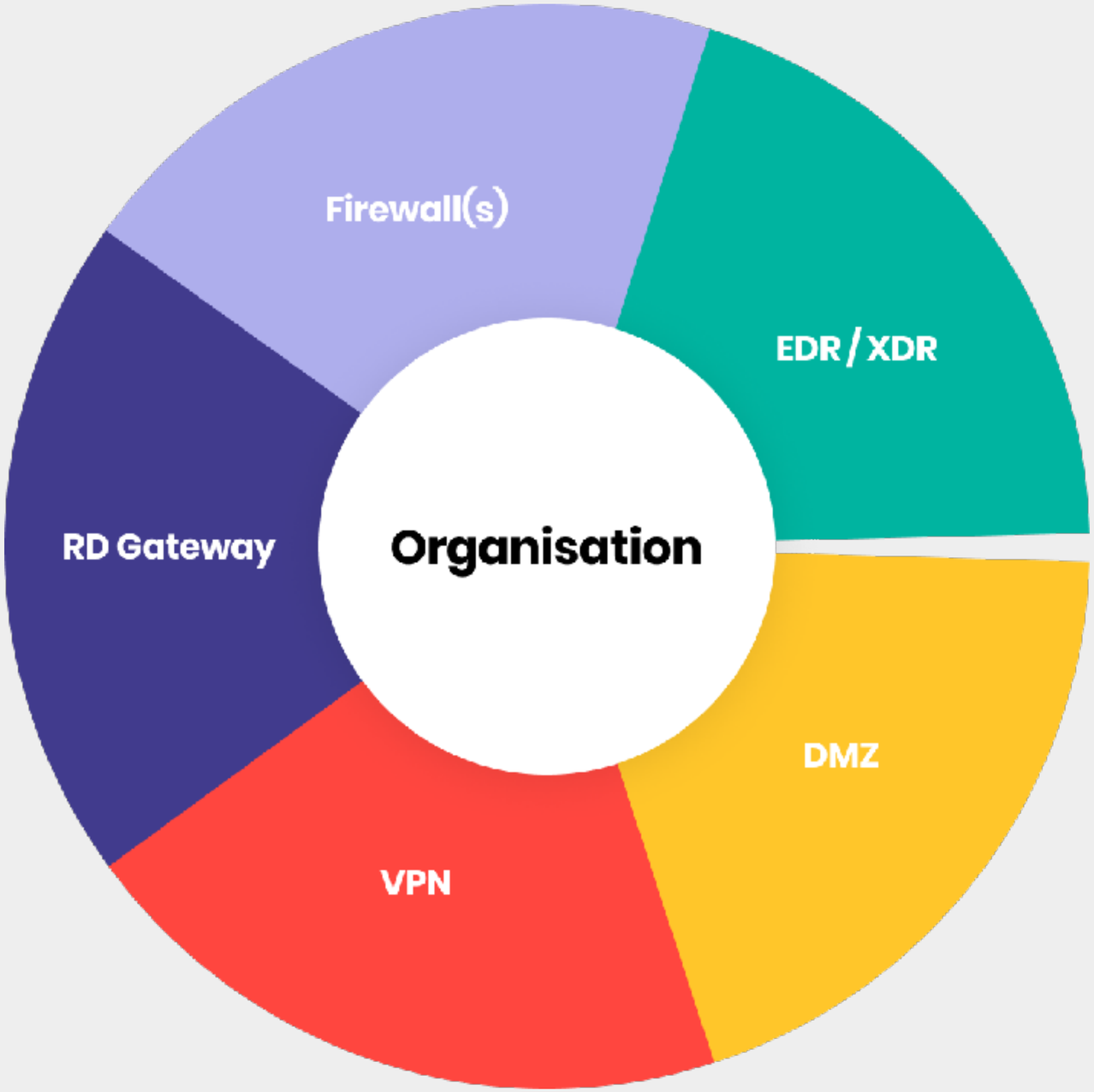
VYŠŠÍ REŽIM

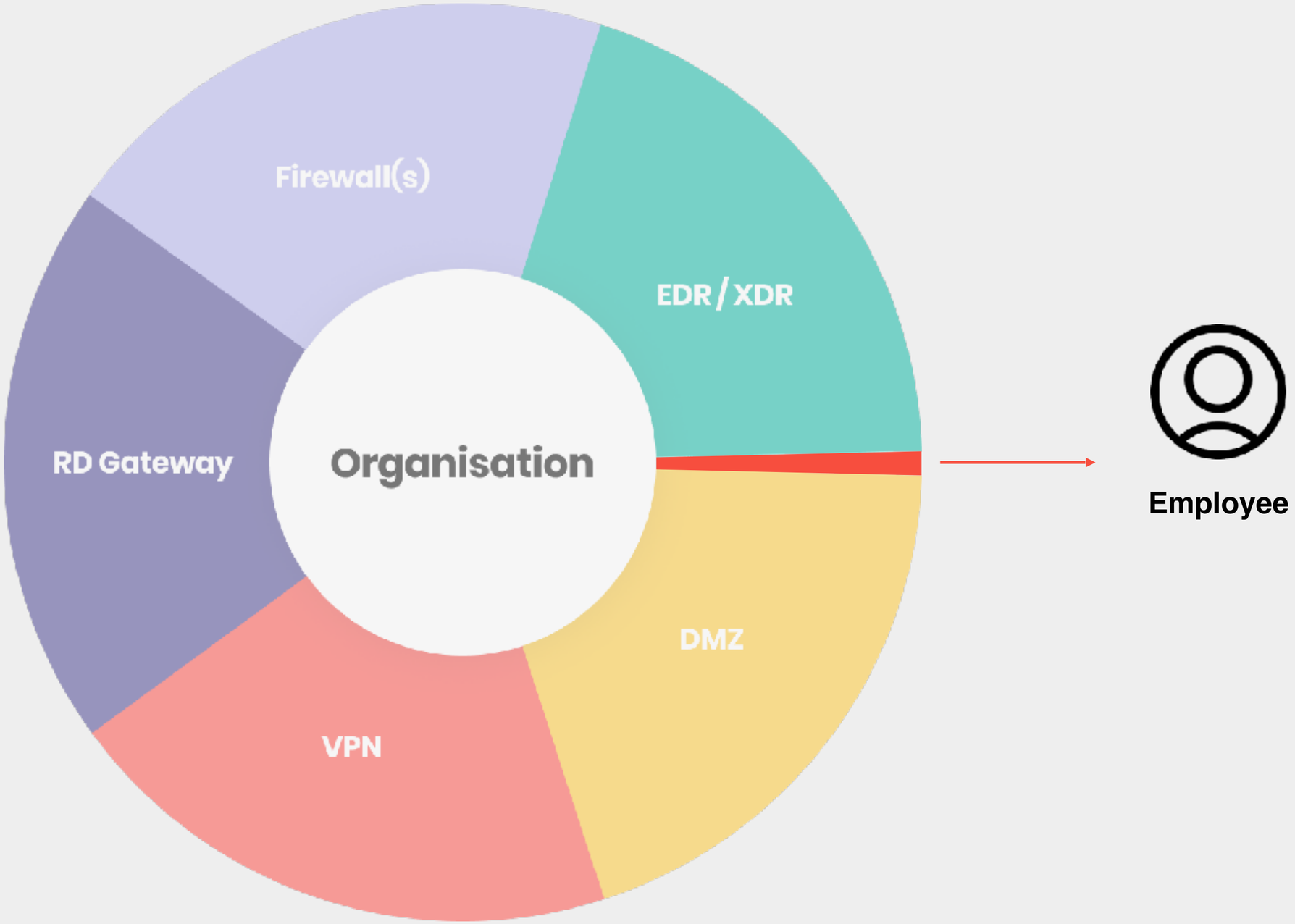
- Přístup na základě rolí (tj. používá Identity Management - IdM)
- **Více-faktorovou autentizaci** nebo
  - autentizaci založenou **na modelu nulové důvěry**
- Přechodně hesla (12/17/22-64 znaků)

Model nulové důvěry

- **Neustálé ověřování** (*Continuous verification*):
  Uživatelé a zařízení jsou ověřování při každém pokusu o přístup – nejen jednorázově při přihlášení.
- **Omezený přístup** (*Least privilege*):
  Přidělují se jen minimální práva potřebná ke konkrétní činnosti.
- **Segmentace** (*Microsegmentation*):
  Síť a aplikace se dělí na menší části, mezi nimiž je samostatné řízení přístupu.
- **Ověření zařízení (***Device trust*):
  Přístup se povolí jen známým, zabezpečeným a řízeným zařízením.
- **Kontextová bezpečnost** (*Contextual access*):
  Oprávnění se posuzují podle: identity, času, polohy, typu zařízení, rizikových vzorců chování atd.






Firewall(s)
EDR / XDR
RD Gateway
Organisation
DMZ
VPN
Employee

Phishing, (Smishing, Vishing, Quishing)

Password Spraying

Spoofing

Credential Stuffing

Ransomware

Man-in-the-Middle

Keylogging

Supply Chain Attack

Brute Force Attack

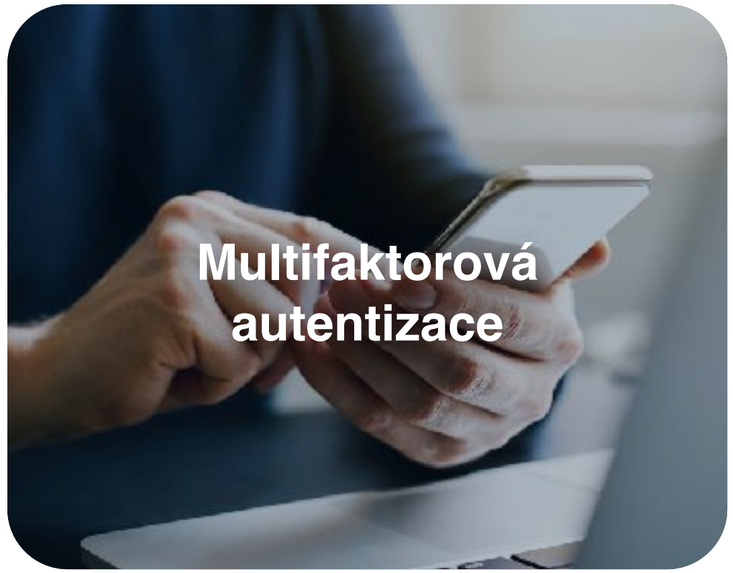
Digital Identity

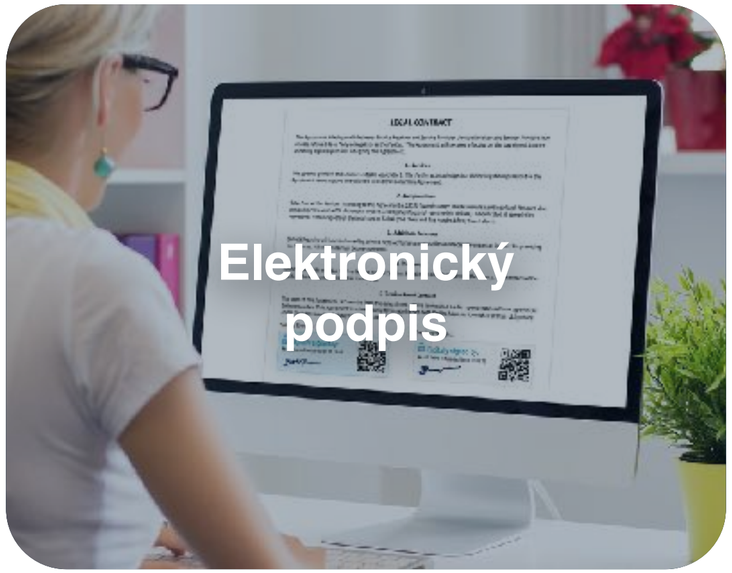
Workforce

Digitální identita zaměstnance

Platforma pro správu

Identit ástrojů Certifikátů





Denní rutina zaměstnance

Multifaktorová autentizace

Přihlášení do OS

Windows macOS Linux

Tool 1

Vzdálený přístup k datům - VPN, RDP

VPN cisco paloalto FORTINET GoodAccess Surfshark OPENVPN CHECK POINT NordVPN

Tool 2

Přihlášení do aplikací třetích stran

ATLASSIAN salesforce Microsoft 365 Google senhasegura GitHub slack YOUR APP

Tool 3

Přihlášení do admin. aplikací

CHECK POINT f5 FORTINET CAS CYBERARK The Identity Security Company

Fyzický přístup

Tool 4

Řízení přístupů




Ovládání přístrojů




Další



Elektronický Podpis

Tool 5

Elektronický podpis - eIDAS 2

PDF On the GO

Denní rutina zaměstnance

Multifaktorová autentizace

Přihlášení do OS

Windows macOS Linux

Vzdálený přístup k datům - VPN, RDP

VPN cisco paloalto FORTINET GoodAccess Surfshark OPENVPN CHECK POINT NordVPN

Přihlášení do aplikací třetích stran

ATLASSIAN salesforce Microsoft 365 Google senhasegura GitHub slack YOUR APP

Přihlášení do admin. aplikací

CHECK POINT f5 FORTINET CAS CYBERARK The Identity Security Company

ProID

Fyzický přístup

Řízení přístupů

Ovládání přístrojů

Další

Elektronický Podpis

Elektronický podpis - eIDAS 2

PDF On the GO

User experience

Security

Možnosti ověření uživatele

Vícefaktorové přihlášení nahrazuje používání uživatelského jména a hesla
nástroji pro bezpečné, šifrované přihlášení s přidáním dalšího faktoru - biometrika, PIN apod.

Jméno / Heslo

Snadné prolomení
či zcizení

Jméno / Heslo
+ další faktor (ProID)

Doplnění o bezpečnostní prvek

Passwordless

Nejvyšší stupeň
zabezpečení

solutions by MONET +

Metody a nástroje k zabezpečení identity

TOP MANAGEMENT

IT Správci

VÝROBA

Kancelář

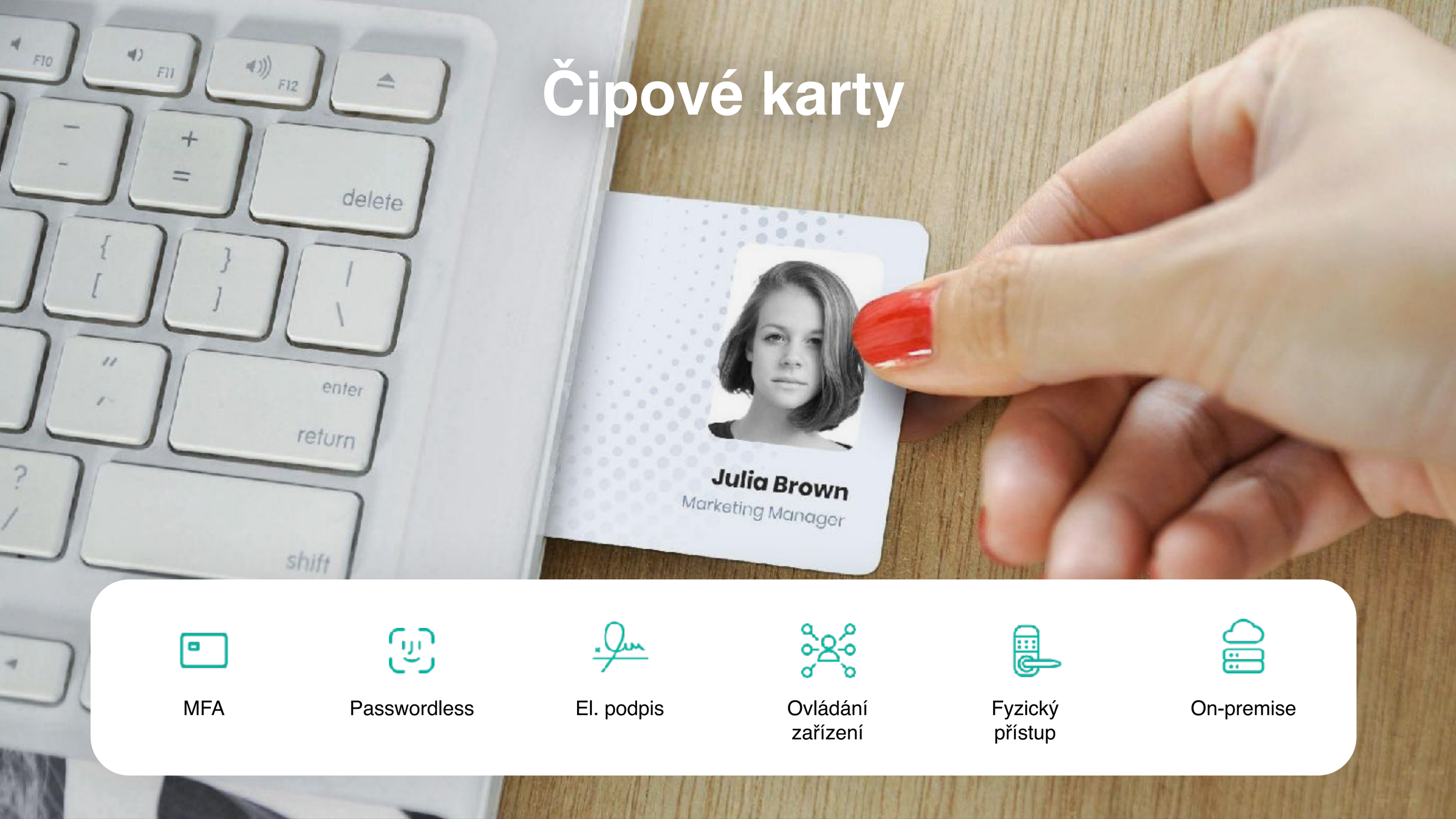
Externisté

Sídlo společnosti

Remote zaměstnanci

Dodavatel

Čipové karty



MFA

Passwordless

El. podpis

Ovládání zařízení

Fyzický přístup

On-premise

Čipové karty

Univerzální a často využívaný nástroj zaměstnance

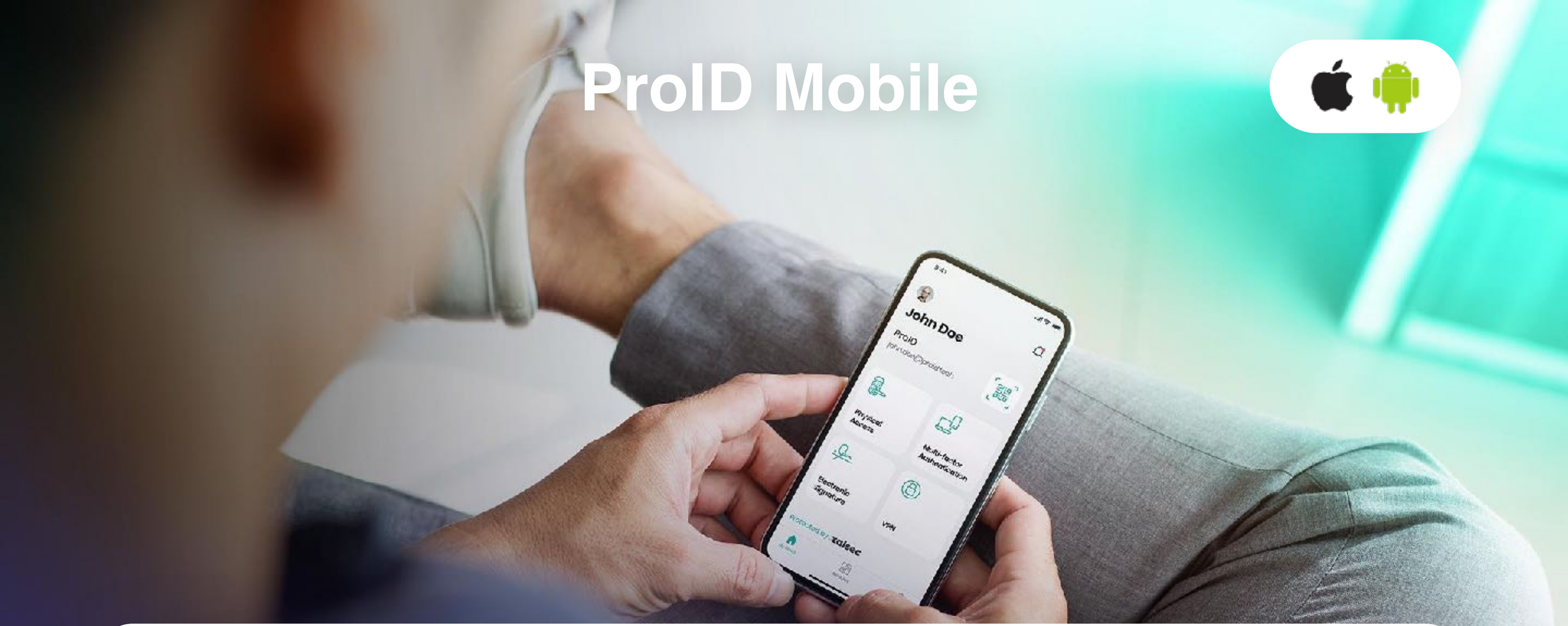
Případy užití:

- Vizuální identifikace
- Bezpečné přihlášení do systémů a aplikací
- Kvalifikovaný elektronický podpis / pečeť (QSCD)
- Fyzický přístup a ovládání zařízení

- **Podpora různých bezkontaktních technologií**
- **Na míru vyrobené hybridní / duální čipové karty** pro potřeby zaměstnanců
- **Vlastní “perso lab”** pro personalizaci karet
- **PKI jako stavební kámen důvěry a bezpečnosti**

fido NXP HID
MIFARE LEGIC 2N

ProID Mobile



MFA

Passwordless

El. podpis

Zabezpečení

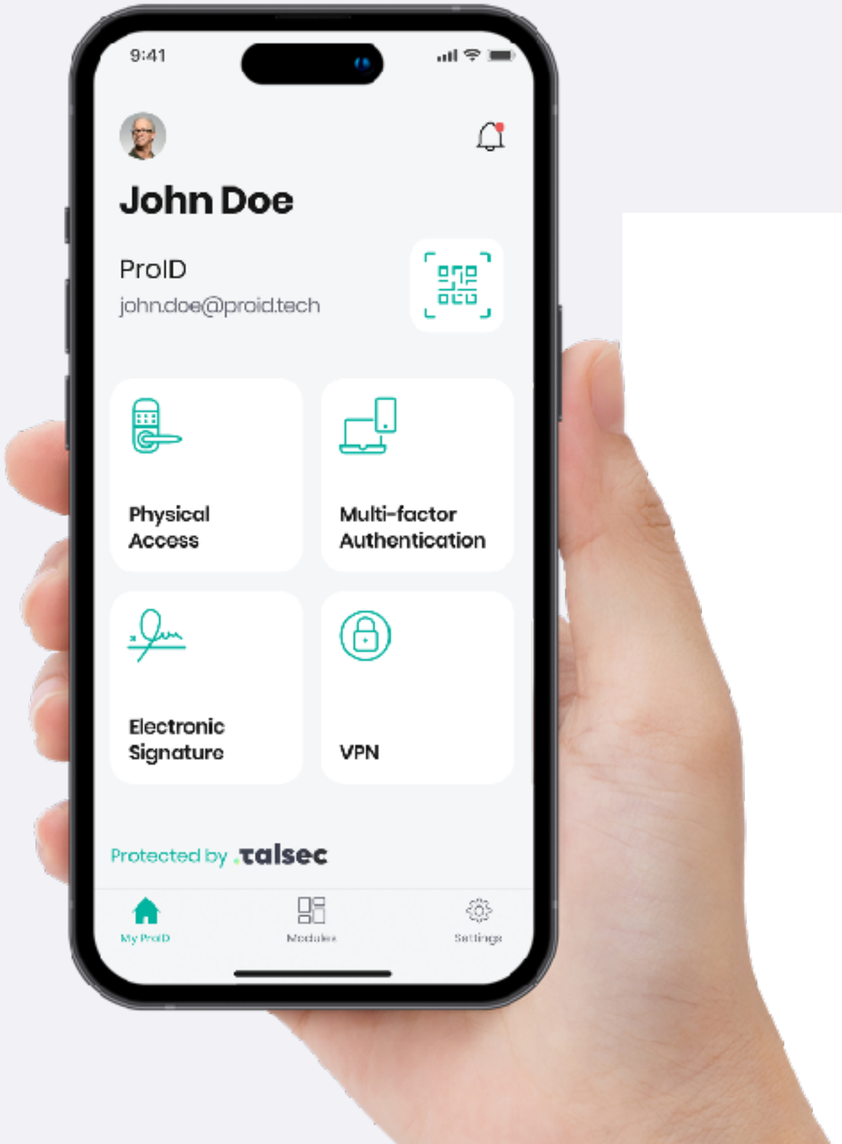
SaaS /
On-premise / Hybrid

Vlastní
produkt

ProID Mobile

Perfektní kombinace elegance, nejnovějších technologií a bezpečnosti

- **“Ultimátní Workforce Aplikace”**
  - jedna aplikace, která vyřeší veškeré bezpečností potřeby zaměstnance
  - výkonná, komplexní a jednoduchá na použití
- **Multifaktorová autentizace “kamkoliv”**
  - využitím standardních protokolů a certifikátů (PKI)
  - passwordless přístup(biometrie nebo PIN)
- **Vzdálený elektronický podpis**
- **Fyzický přístup / ovládání přístrojů**
  - emulace bezkontaktních čipů pomocí BLE / NFC
- **Bezpečnost**
  - kontrola aplikace / zařízení v reálném čase – “RASP”
  - PIN policy



Způsoby ověření na mobilu

Push notification
(mobilní token)

Jednorázové heslo
(One Time Password)

SMS
s autorizačním kódem

Anonymní
QR kód

solutions by MONET+

Autentizační protokoly

RADIUS protocol

PASSWORDLESS

Federate protocols
SAML 2.0 / OIDC
OAuth 2.0

PASSWORDLESS

Certificate-Based
PKI

Zdroj identit

Azure AD

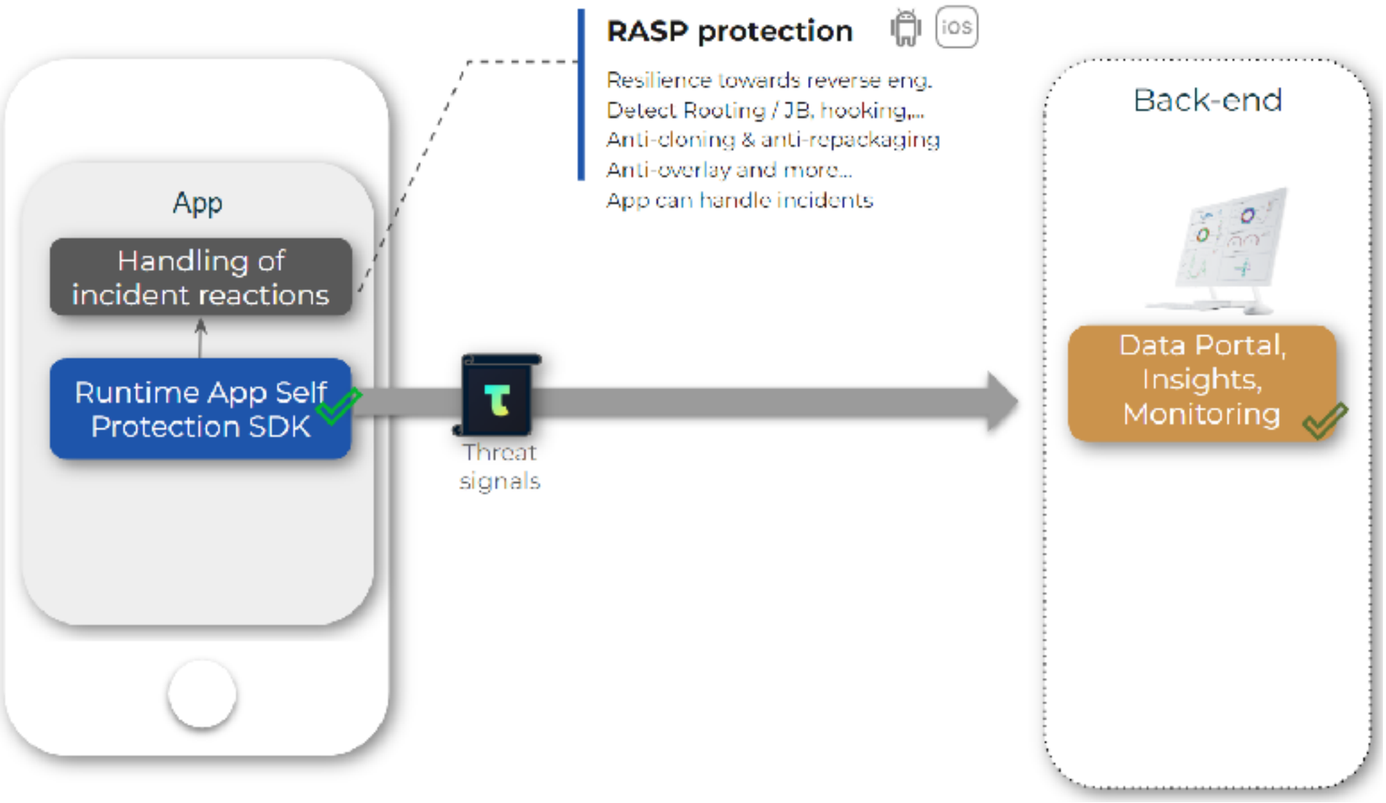
Active Directory

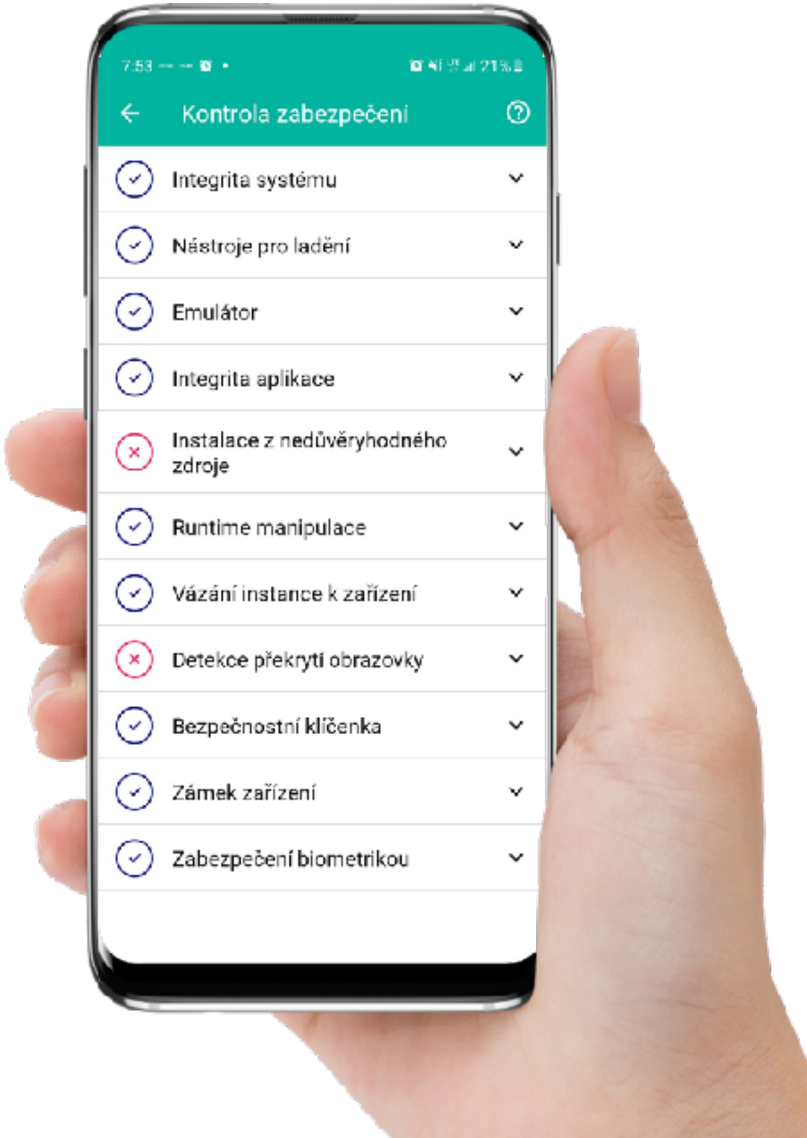
IAM Connect API

Zvýšená bezpečnost v mobilní aplikaci

RASP (runtime application self-protected) integrované SDK

pro vyhodnocování nebezpečí v mobilní telefonu - **Talsec.app**





Přihlášení do operačního systému

Windows

PASSWORDLESS

Zdravotnictví

60 nemocnic

Finančnictví a telekomunikace

5 největších bank
3 mobilní operátoři

Veřejná správa

5 ministerstev
30 měst
6 krajských úřadů

Kritická infrastruktura

Výrobci energie
Distributoři energie

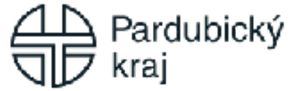
Výroba

Automobilový a potravinářský průmysl


STC


ČSSZ


Vyškov


Pardubický
kraj


NEMOCNICE
ČESKÉ BUDĚJOVICE, a.s.


orange


Úřad práce ČR


ČESKÁ
spořitelna


FAKULTNÍ NEMOCNICE
OLOMOUC


KB


Rýmařov


ČSOB


Olomoucký kraj


MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY


O2


UniCredit Bank


oncomed


Kooperativa
VIENNA INSURANCE GROUP


MASARYKŮV ONKOLOGICKÝ ÚSTAV

Ondřej Mareček

Sales Manager

omarecek@monetplus.cz

+420 605 535 923

proid.cz | monetplus.cz

Děkuji!