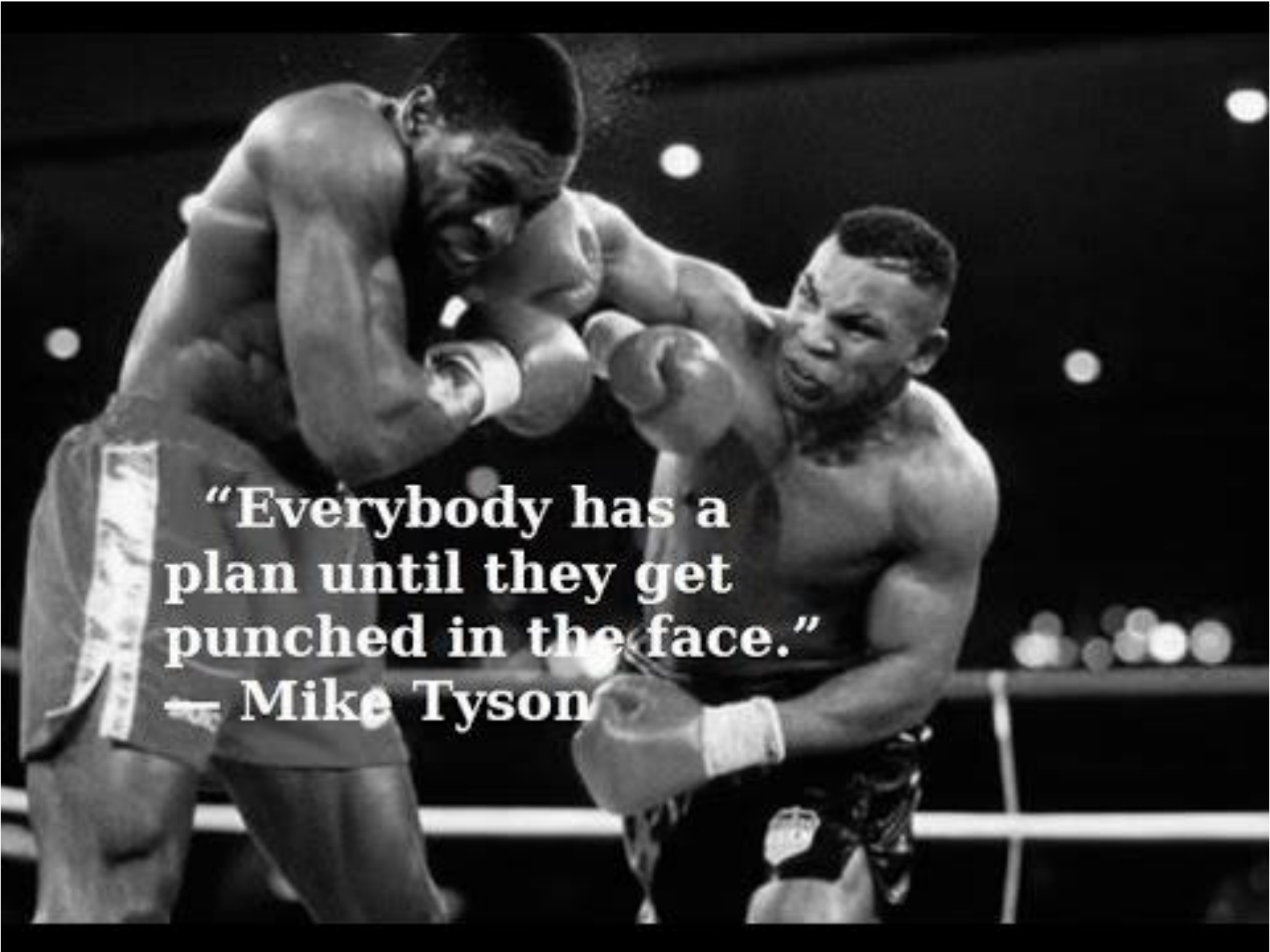


┌ Az identitás az új...minden!

Passwordless? User persona?
Autentikációs utak?
MFA? PKI? IAM? CIAM?

Paksi Attila, Thales, 2022 október 18
Nádor IT biztonsági partner nap





**“Everybody has a
plan until they get
punched in the face.”
— Mike Tyson**

A Ransomware megváltoztatta az adatlopások gazdaságosságát



19%

of organizations said they **had been the target** of a ransomware attack



55%

have no formal plan to follow in case of a ransomware attack



20%

of respondents said they **would pay or have paid a ransom** for their data



Phaas

Mi az a PhaaS?

- On May 2022, a new service by **EvilProxy** has emerged, promising to steal authentication tokens to bypass multi-factor authentication (MFA) on Apple, Google, Facebook, Microsoft, Twitter, GitHub, GoDaddy,
- **Zero code phishing solution** for the low-skill threat actors
- EvilProxy is offered on a **subscription** base - 10, 20 or 31 days
- Attackers get : user credentials and an authenticated session cookie
- Available both in the clearnet and darknet

Mennyibe kerül a PhaaS?

Contacts: evilproxy

Available Services & Prices

Account Balance: 400

Search for

Bundle	Entry Scopes	Data Collected	Price
 dropbox	dropbox.com	✓ login	10 days - 150\$
		✓ password	20 days - 250\$
		✓ session cookies	31 days - 400\$
 rubygems	rubygems.org	✓ login	10 days - 150\$
		✓ password	20 days - 250\$
		✓ session cookies	31 days - 400\$
 yandex	yandex.ru	✓ login	10 days - 150\$
		✓ password	20 days - 250\$
		✓ session cookies	31 days - 400\$
 yahoo	yahoo.com	✓ login	10 days - 150\$
		✓ password	20 days - 250\$
		✓ session cookies	31 days - 400\$
 microsoft	xbox.com		
	skype.com		
	onenote.com		
	office.com	✓ login	10 days - 150\$
	microsoftonline.com	✓ password	20 days - 250\$
	microsoft.com	✓ session cookies	31 days - 400\$
	live.com		
bing.com			
		✓ login	10 days - 150\$

Who's Twilio

- Based in San Francisco
- 8510 employees
- Provides programmable communication tools
- ~250,000 customers



The phishing attack

- Aug 1st-10th
- Twilio used [REDACTED]'s Single Sign-On product
- The URLs used words including 'Twilio,' '[REDACTED],' and 'SSO' to trick users
- Attackers gained access to Twilio's customer support console
- Aftershoc: Signal breach, remediation...

Who's Cloudflare

- Based in San Francisco
- An American content delivery network and DDoS mitigation company
- It primarily acts as a reverse proxy between a website's visitor and the Cloudflare customer's hosting provider



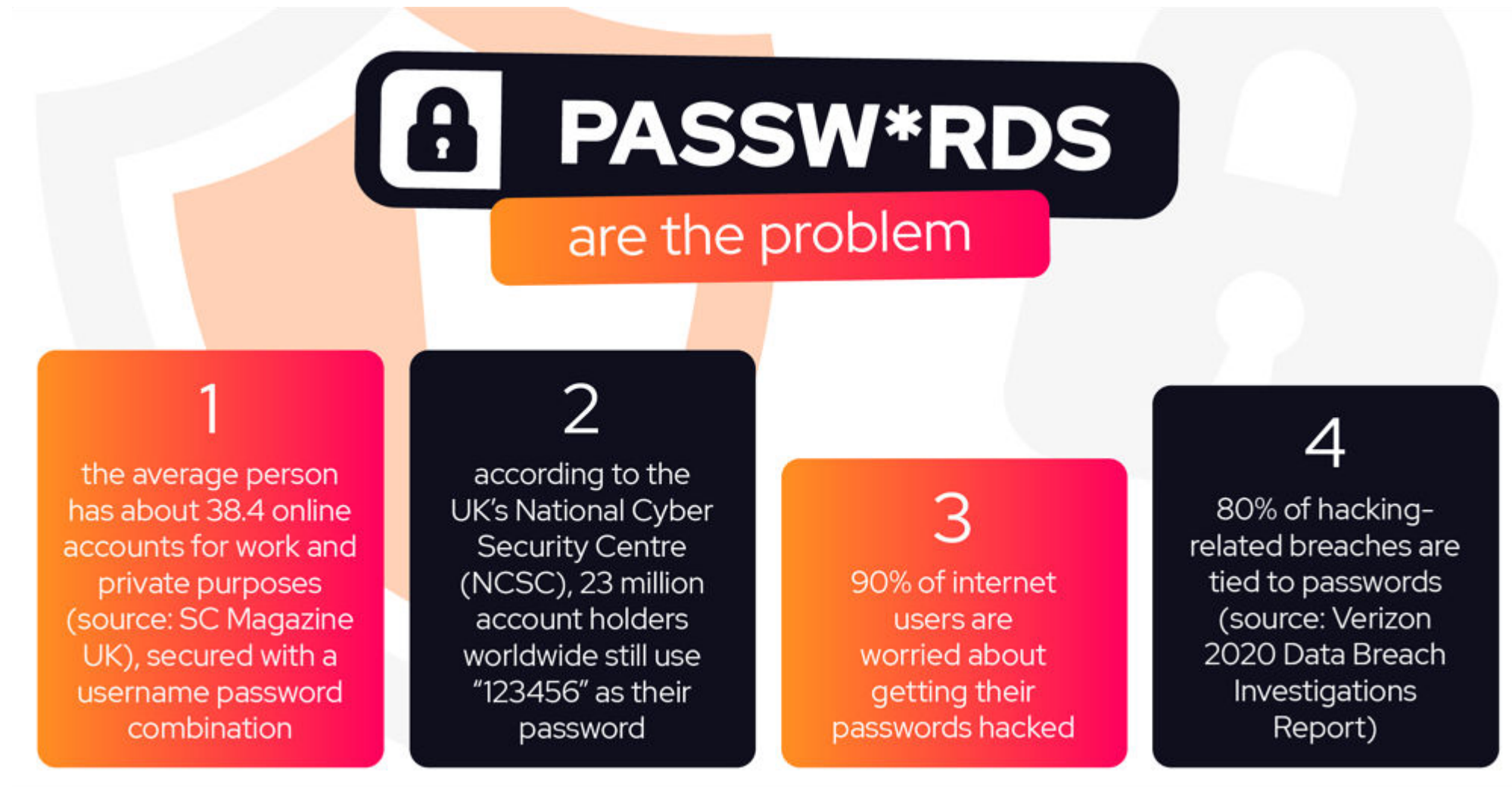
CLOUDFLARE®

THALES

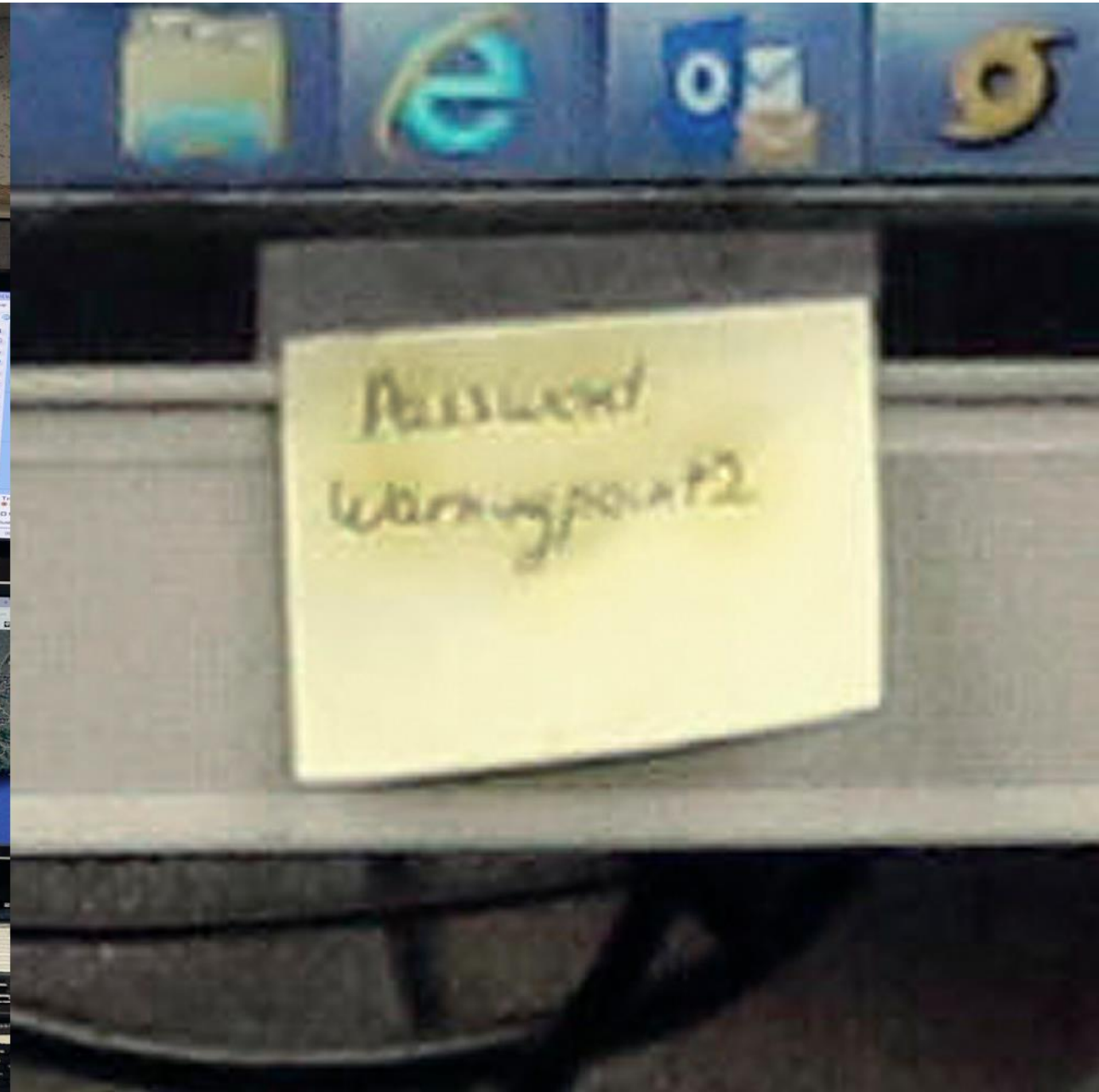
The Cloudflare's attack

- On July 20, 2022, the Cloudflare Security team received reports of employees receiving legitimate-looking text messages pointing to what appeared to be a Cloudflare  login page
- Employees and family members received text messages
- Spoof login website was registered less than 40 minutes before the phishing campaign began
- Every employee at the company is issued a **FIDO2-compliant token**
- Attack result: NONE 😊

A jelszó rossz, értem?



Ez egy SOC...

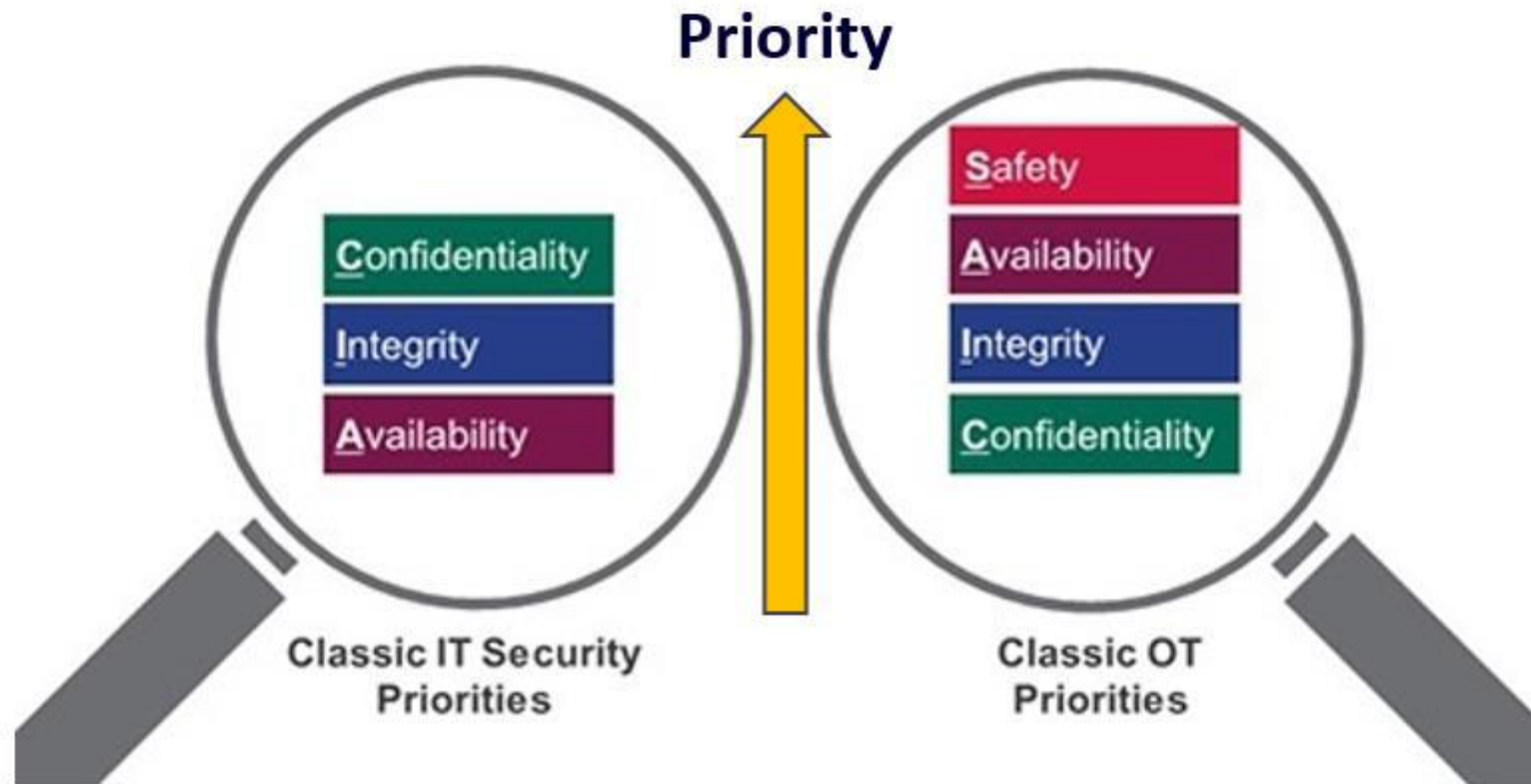


A CISA 16 kritikus infrastruktúráis szektort azonosított



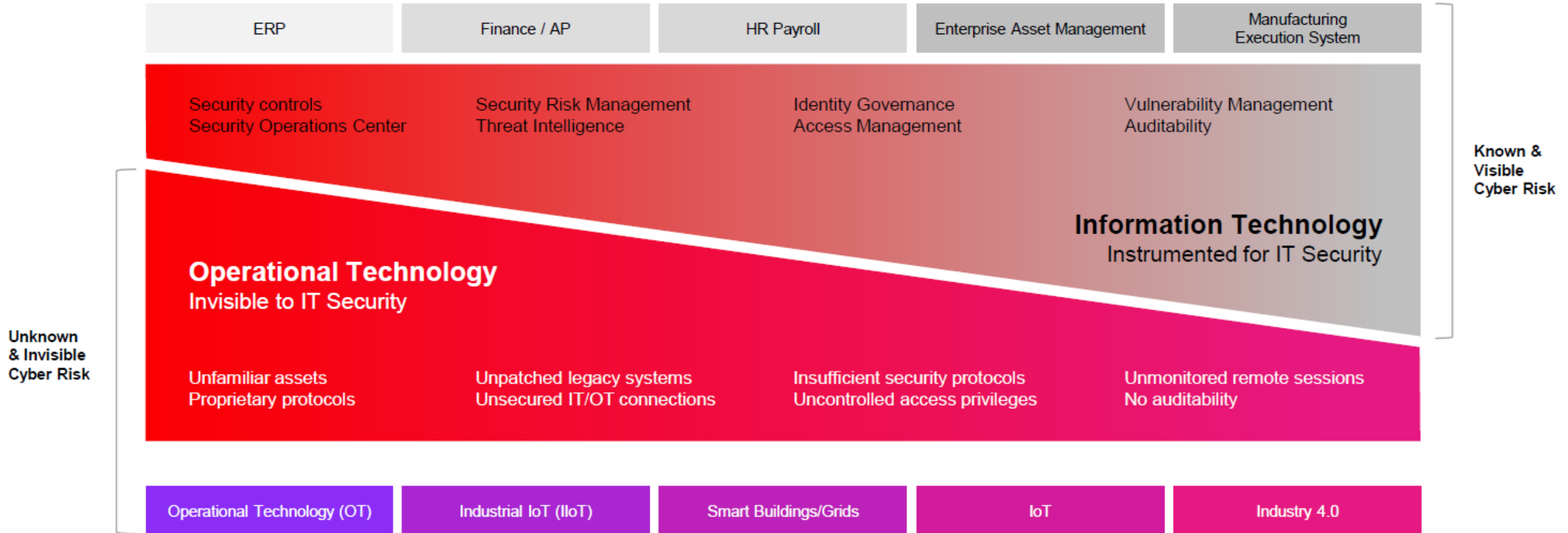
CISA
CYBER+INFRASTRUCTURE

IT vs OT prioritások

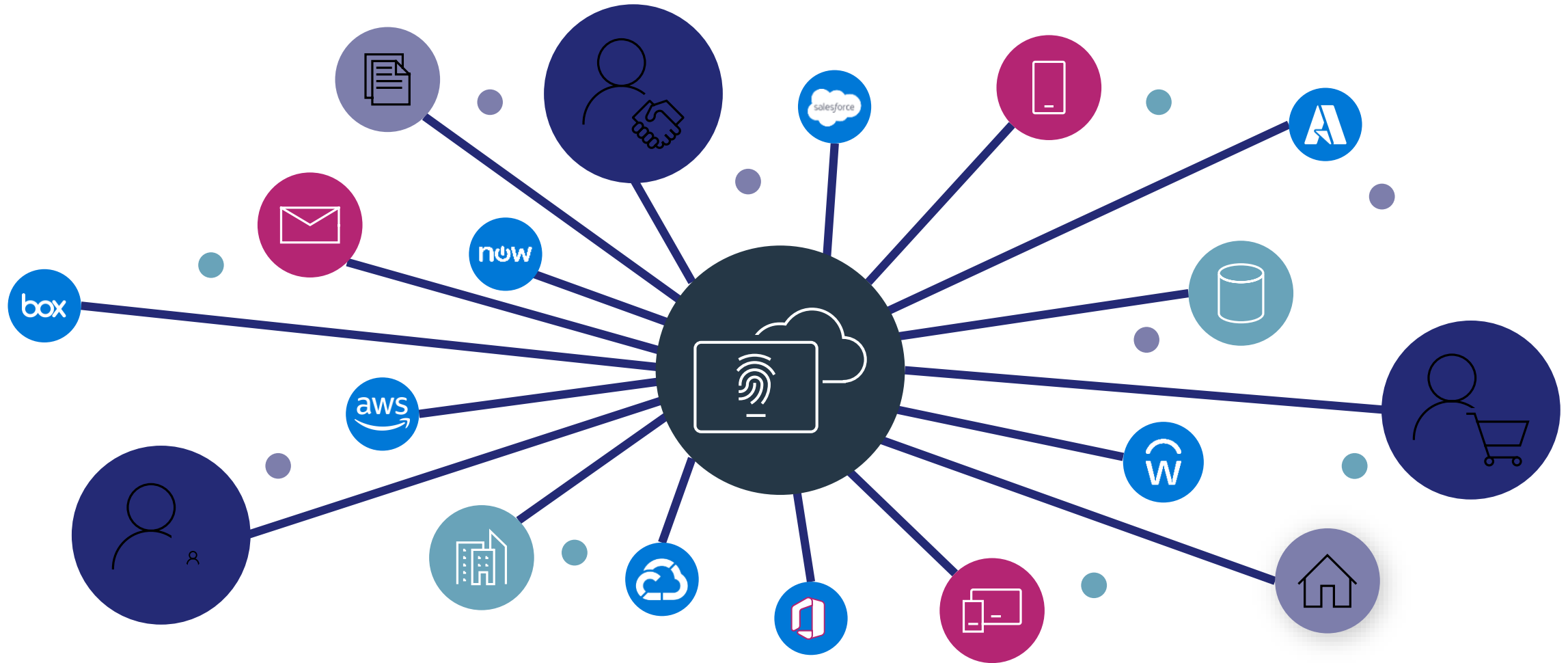


Can't protect what you can't see

A High Inherent Cyber Risk to Process Resiliency - OT risk is invisible to IT security



Az identitás a központi vezérlő sík



ZERO TRUST POLICY



Zero Trust stratégia

Nincs hivatalos Zero Trust stratégia

21%



Zero Trust stratégia a tervezési és keresési szakaszban

26%

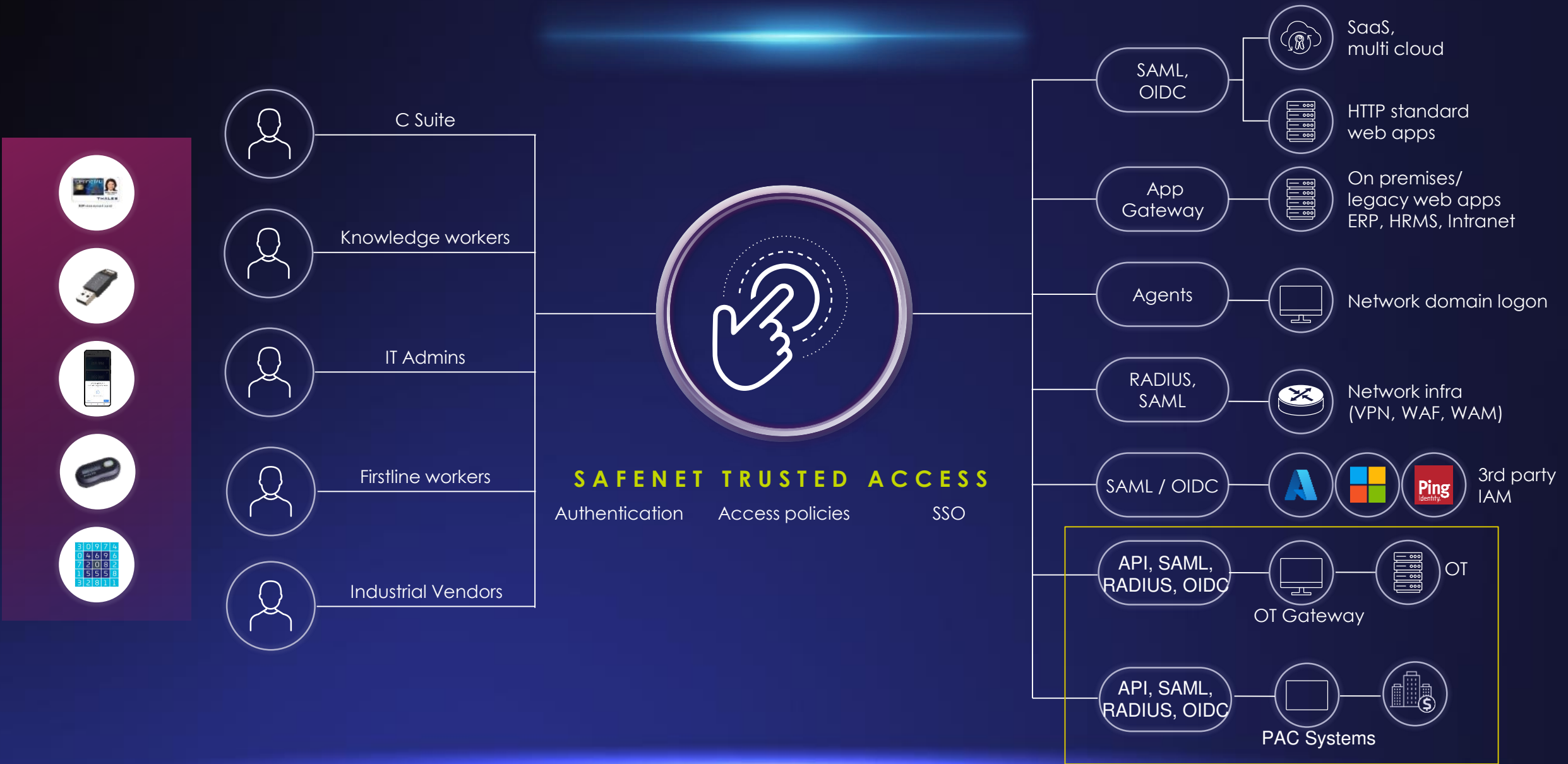


Aktívan elfogadott irányelvek és hivatalos Zero Trust stratégia

30%



HOW DOES STA PROTECT THE ENTIRE MANUFACTURING ENVIRONMENT?





Hogyan és kinek tegyem
BIZTONSÁGOSAN elérhetővé
távolról is az adatokat?





Discover



Protect



Control

Data Security for a Zero Trust World

A THALES MEGKÖZELÍTÉSE: A HÁROM LÉPÉSES TERV

Discover

IAM Workshop



Határozza meg, kik a felhasználói, és milyen konkrét igényeik vannak a hitelesítési útjaik során.



A szabályozói megfeleléshez szükséges idő lerövidítése



A működési hatékonyság és az üzembiztonság növelése



A biztonsági rések felfedezése és bezárása

Protect

STA szabály- és kockázati motor

“

Védjen meg több felhasználót hozzáférési szabályokkal és erős hitelesítéssel.



Az érzékeny adatok védelme egyetlen lépésben, manuális beavatkozás nélkül



Proaktív védelem a sebezhetőség és kockázati profil alapján



Egységes védelem és magas szintű adatbiztonság a hibrid IT-környezetekben

Control

Az irányelvek érvényesítése
és nyomon követése



A kockázatok nyomon
követése és ellenőrzése
valós idejű, folyamatos
szabályzat-érvényesítéssel



Biztosítsa az összes
felhasználói utat erős
hitelesítési lehetőségekkel



Legyen saját és egységes
hozzáférés- és
adatbiztonsága



Szabályzat alapú,
kockázatarányos
hozzáférés kezelés

Mire figyelünk technológia szempontból?

- Csak a **VPN-hez** kell, vagy van más **use case-ünk is?**
- Segítenék az **automatizációk** az adminisztrációt?
- Mennyire **biztonságos** a tokenek kiadása?
- Függhetnek-e **csak egy (felhő) szolgáltatótól??**
- ...

Mire figyeljünk üzleti szempontból?

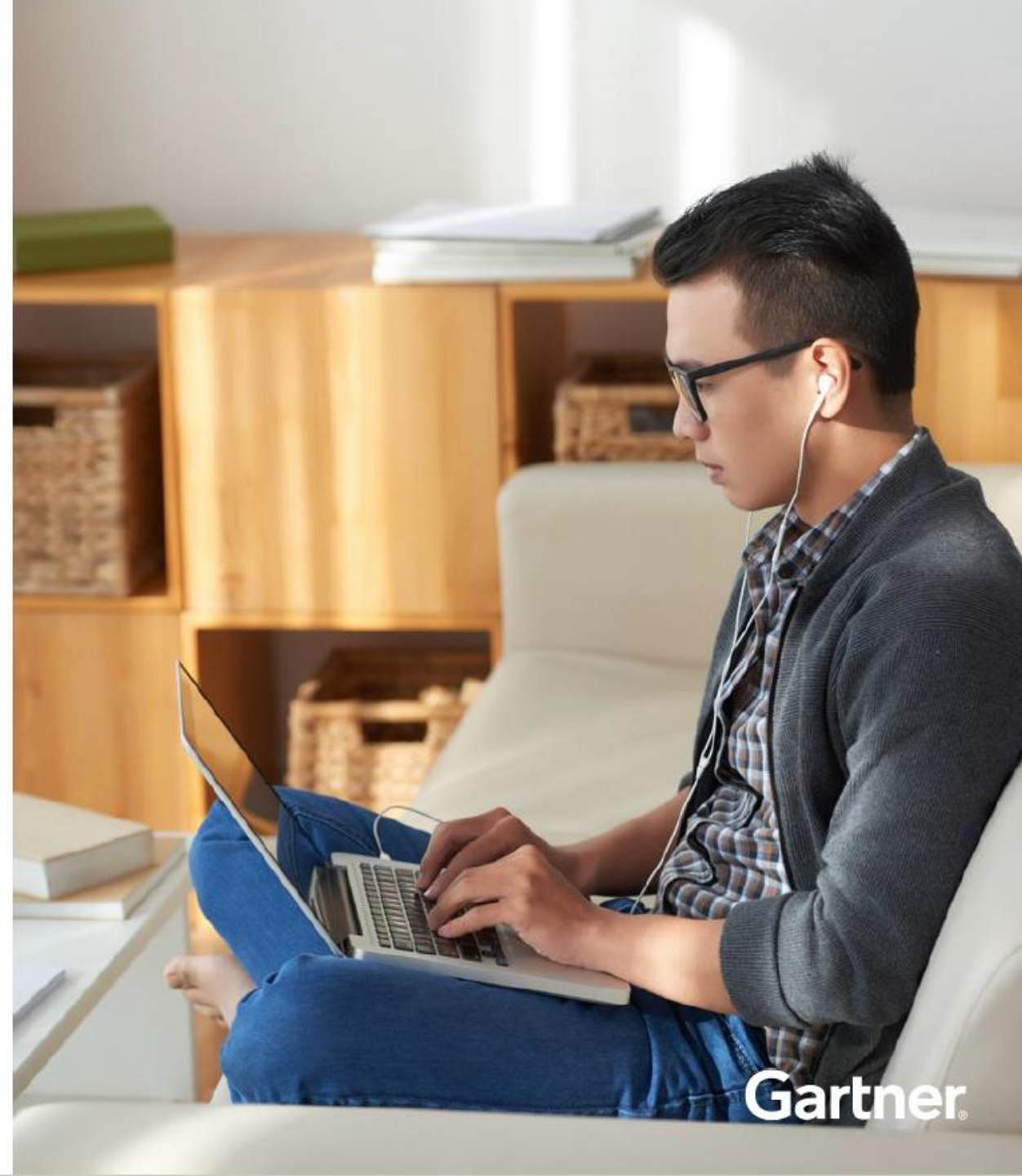
- Mit kell **TCO**-mba beleszámítanom? Transzparenssek a költségeim?
- Van **elég kolléga** egy IAM-megoldás bevezetéséhez és üzemeltetéséhez?
- Külön **szabályokra** van szükségem bizonyos alkalmazásokhoz és felhasználókhoz?
- Elegendő **csak egy mobil token** az összes felhasználómnak?
- ...

**A felhasználók NEM
egyenlőek...**

User Experience Matters

- Adding MFA can add friction (but it doesn't have to)
- Employee and customer experience is more important than ever
- Offering multiple options for diverse users is necessary
- Password less MFA is one possible answer

Source: Gartner



User Persona – Hogyan határozhatóak meg?

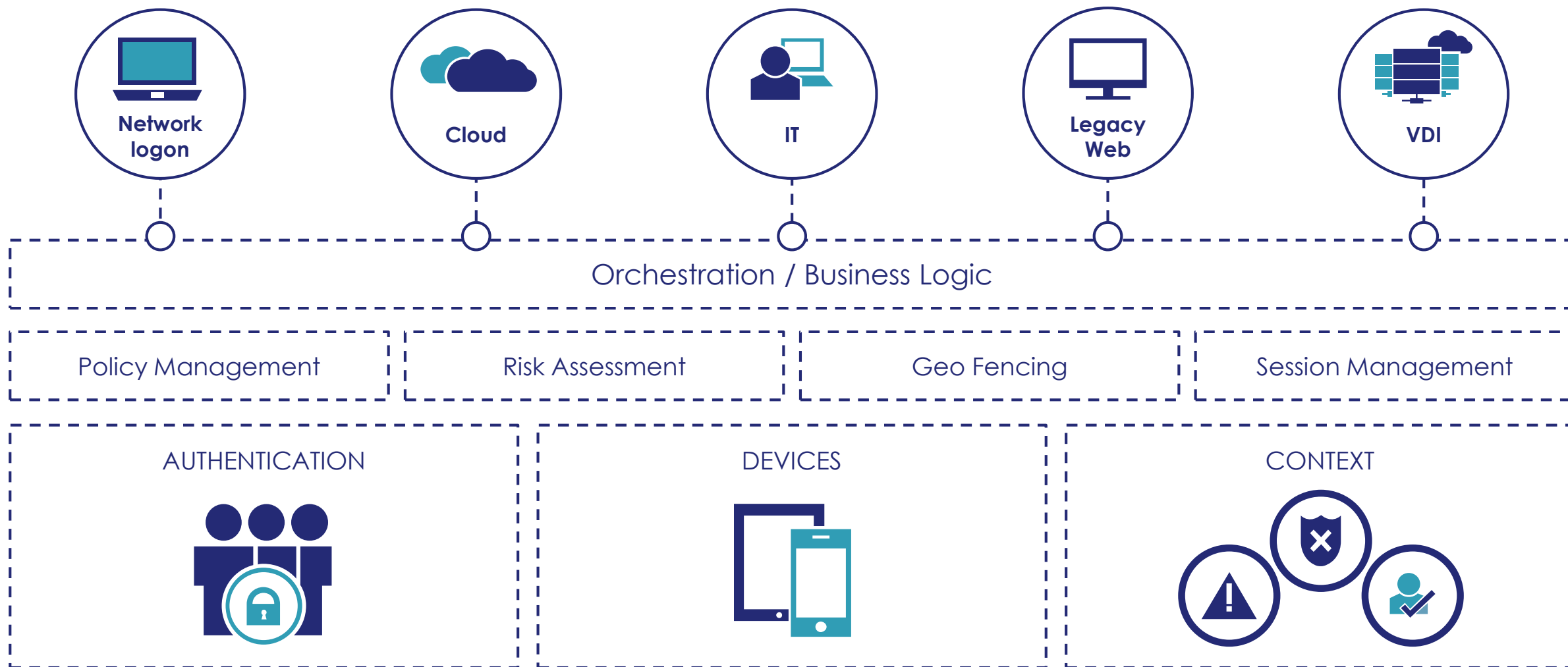
- Jellemzők
- Képességek
- Termékigények
- Célok
- Felszerelés
- Elhelyezkedés
- ...



User Persona – A felhasználók NEM egyenlőek...



A Thales válasza - SafeNet Trusted Access



Univerzális autentikációs lehetőségek



**A meglévő MFA
telepítések
újrafelhasználása**

**A PKI autentikáció
kiterjesztése a
felhőre**

**Az adott
kockázatnak
megfelelő
biztonsági szint
garantálása**

THALES



Új utak - PKI, FIDO, Virtuális smart kártya

www.thalesgroup.com



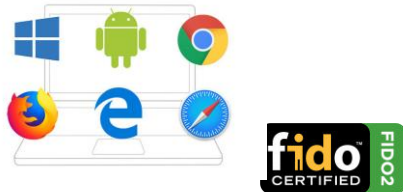
Vezető szereplő a PKI alapú hitelesítés területén

Fejlődés

Új felhasználási esetek támogatása



IDPrime Virtual



FIDO hardver
autentikátorok

Karbantartás

A legerősebb MFA portfólió



Smartkártyák



Tokenek



Middleware

SafeNet IDPrime Virtual

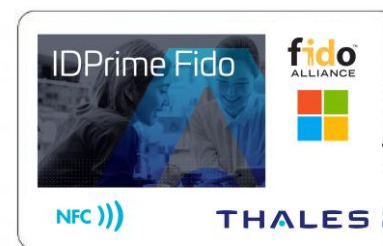
- A fizikai smartkártya szoftver alapú, biztonságos változata
- Csökkenti a fizikai eszközök operatív kihívásait
- Kiterjeszti a tanúsítvány alapú autentikációt és tranzakciókat új felhasználási esetekre:
 - VDI
 - BYOD és mobil eszközök
 - Ideiglenes smartkártyák
 - Könnyű smartkártya pótlás



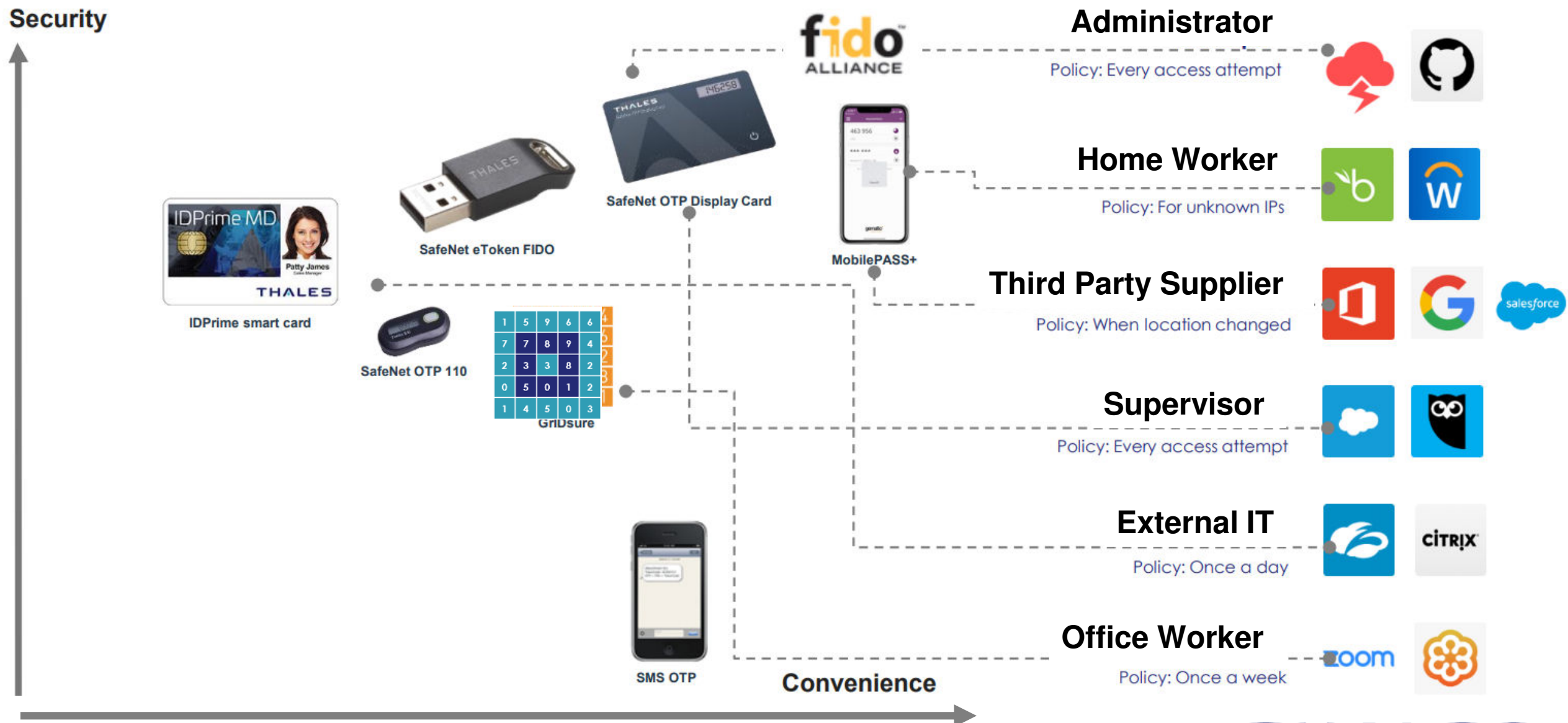
- PKI és FIDO2 támogatás egy eszközben
- Meglévő PKI befektetések felhasználása
- Gyors üzembe helyezés a Thales Middleware és a meglévő PKI infrastruktúra alapján

■ PKI + FIDO2 eszközök

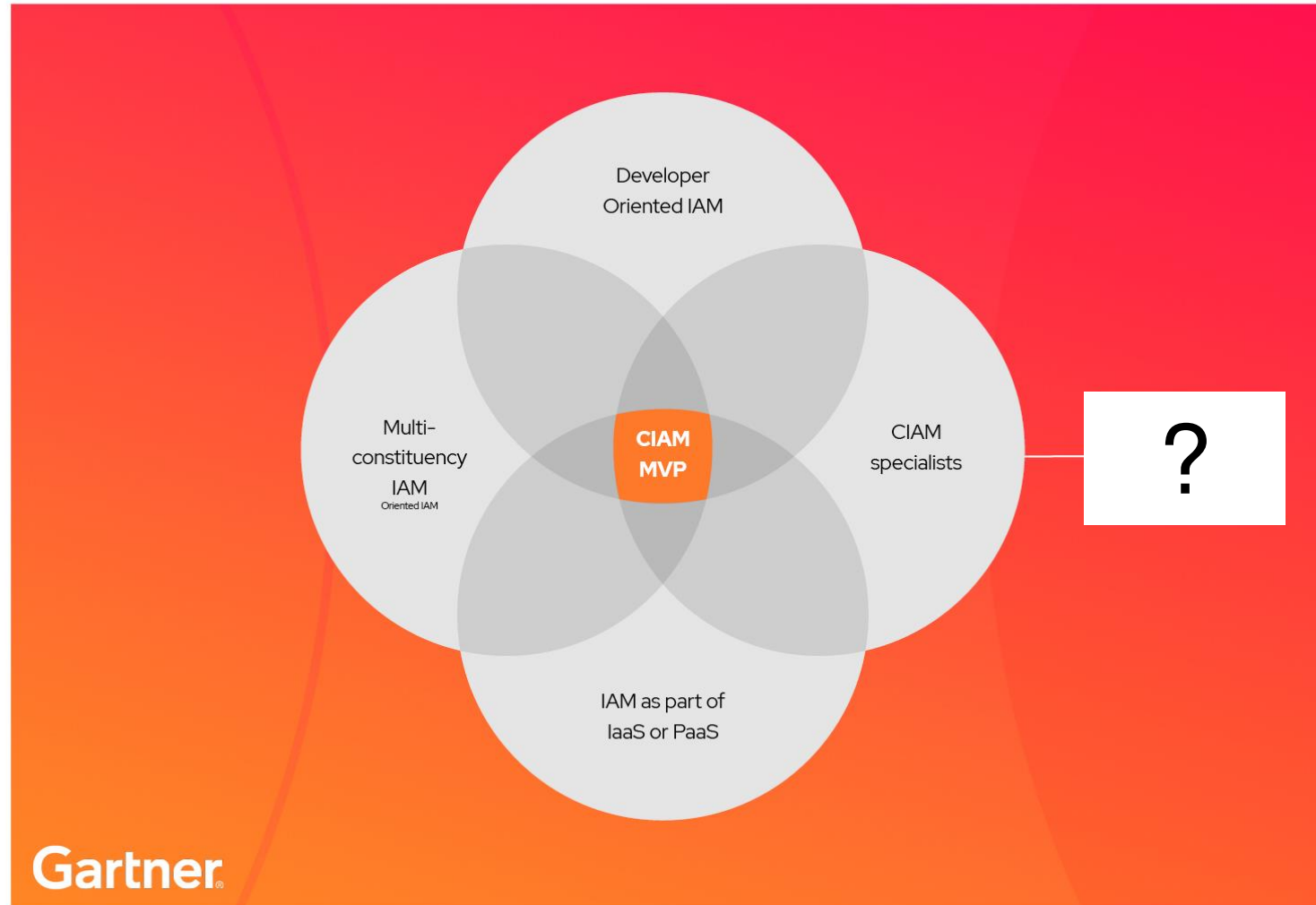
- Kombinált FIDO – PKI Smartkártya
- FIDO USB token



Eltérő autentikációs utak



CIAM – a következő lépés



Technology Insight for Customer Identity and Access Management (11.2021)

onewelcome is now **THALES**



From the Cold side of Identity

where IAM is a hygiene and
costs factor driven by IT only, to

To the Cool Side of Identity!

Where IAM adds value directly
to the business and its customers
Suppliers and partners



IAM vs. CIAM

Which Solution is Right For You?

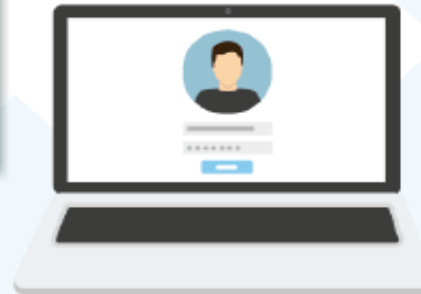
IAM

Internal-facing solution that manages employee identities



CIAM

Consumer-facing solution that manages customer identities on multiple platforms



HOW CAN YOU ENSURE THAT...



EMPLOYEES CAN
SECURELY ACCESS THEIR
APPS WHEREVER THEY
ARE?



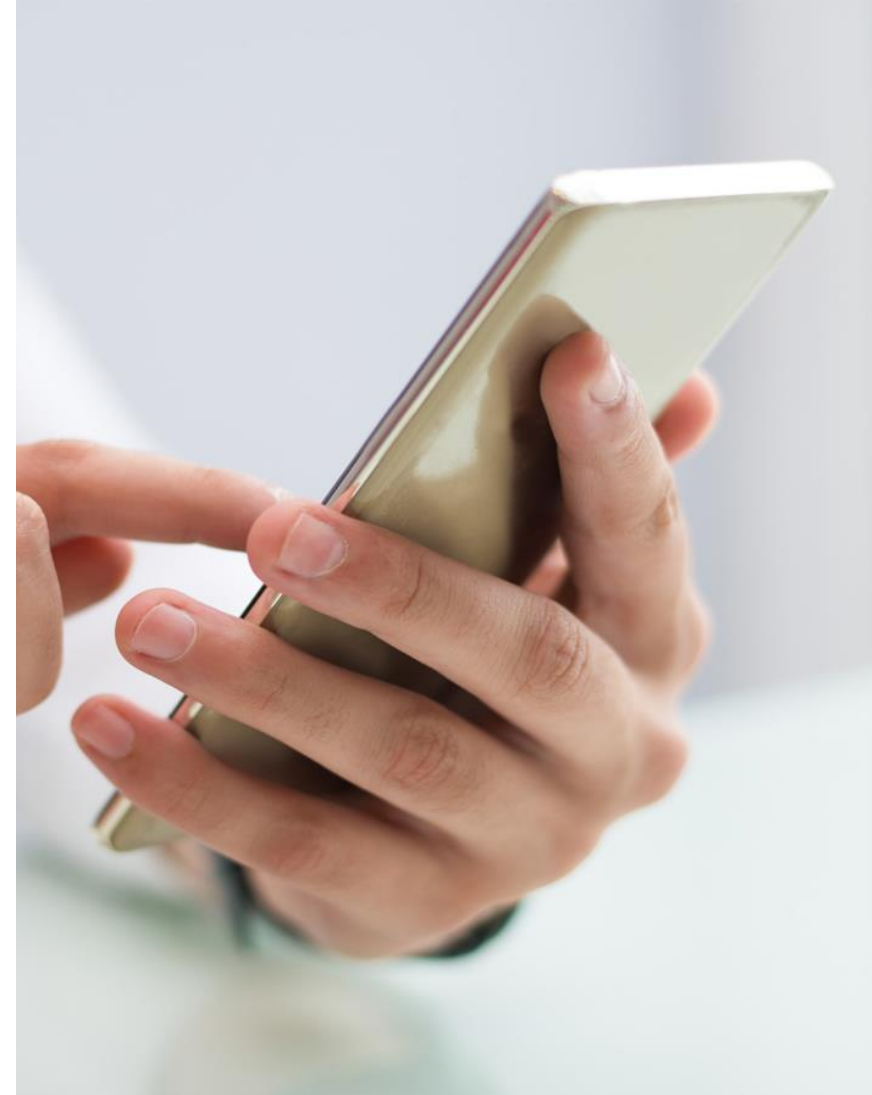
PARTNERS GET EASY AND
SECURE ACCESS TO
THEIR BUSINESS
PORTALS?



GIG WORKERS CAN
QUICKLY ONBOARD
TO NEW PLATFORMS?

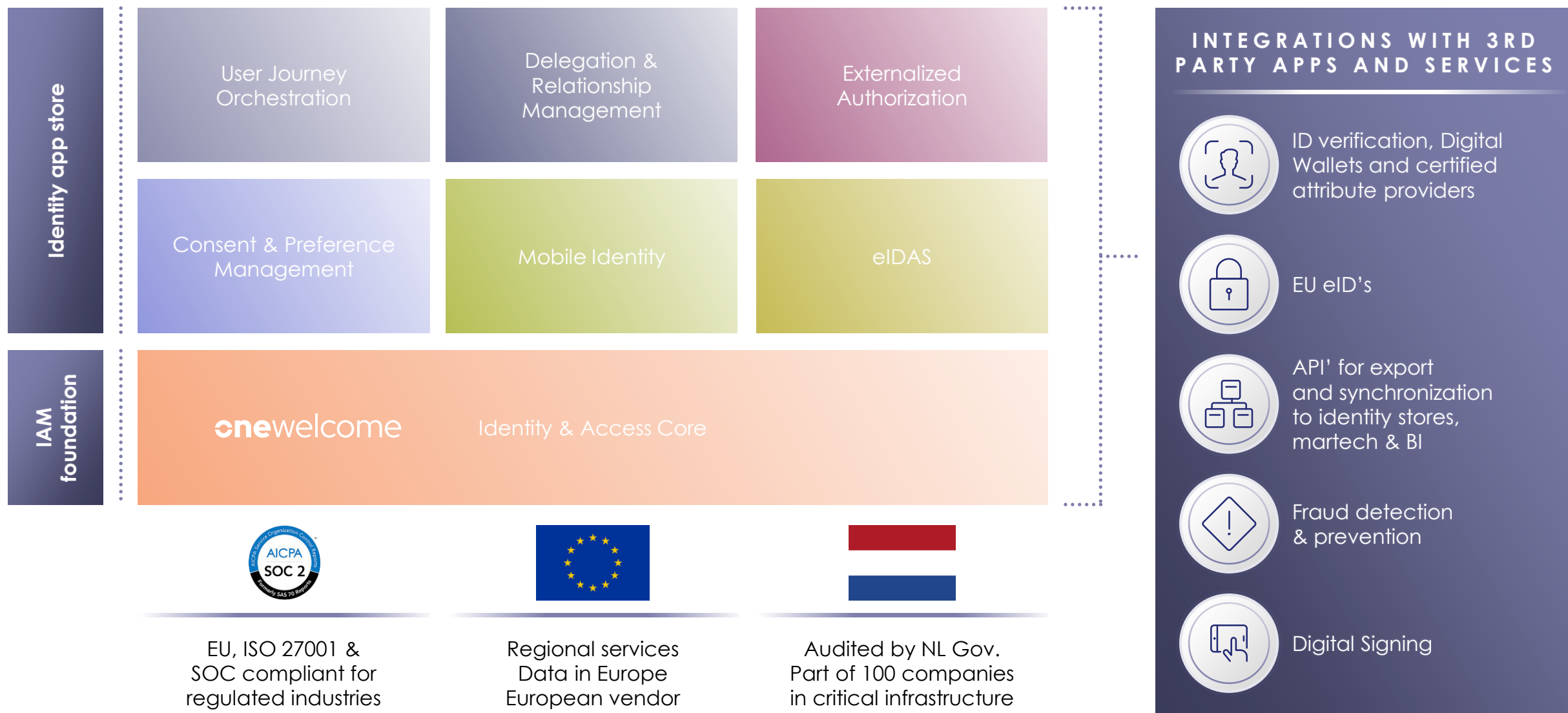


CUSTOMERS CAN
REGISTER AND COMPLETE
PURCHASES SMOOTHLY,
WITHOUT DISRUPTION?

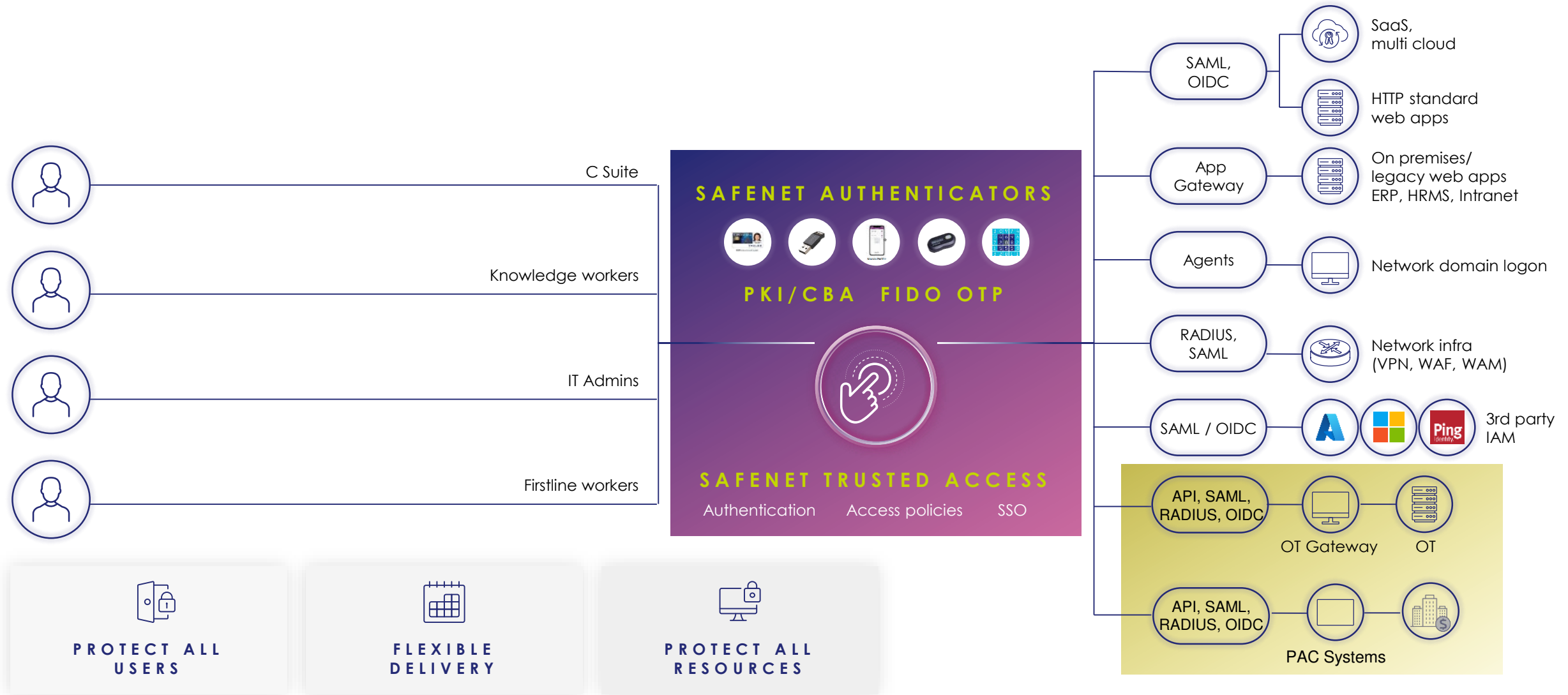


IDENTITY APPS FOR ALL B2C, B2B AND GIG USE CASES

Business identity apps on top of a solid OneWelcome core or augmenting 3rd party IAM



onewelcome : ONE PLATFORM FOR EVERY IDENTITY



“A remény nem stratégia”





Köszönöm a figyelmet!

Paksi Attila

+36 30 202 6000

attila.paksi@thalesgroup.com

Thank you

Gracias مكمل اركش

धन्यवाद Merci

Danke 謝謝

ありがとうございました