# Személyazonosság-kezelési (IDM) projektek tipikus célkitűzései és azok elérése

**Hargitai Zsolt**
üzletfejlesztési vezető
Novell Magyarország
zsolt.hargitai@novell.hu

Novell®

# Miről lesz ma szó?

## Célok és azok elérése

Személyazonosság-kezelés célkitűzései és azok elérésének lehetősége

## Tipikus problémák

Bevezetés során elkövetett tipizálható problémák és azok kivédése

## Szerepkörök és adattisztítás

Szerepkörök kialakításának fontossága, kialakításának módszerei

## Jelentések, PSZÁF elvárások

Jelentések készítése, törvényi- és PSZÁF-megfelelőség elérése

# Komplex kihívások

Hogyan lehet a felhasználókat és azok jogosultságait egyszerűen, mégis dinamikusan nyilvántartani?

Hogyan lehet az IT működését és a végfelhasználók munkáját hatékonyabbá tenni?

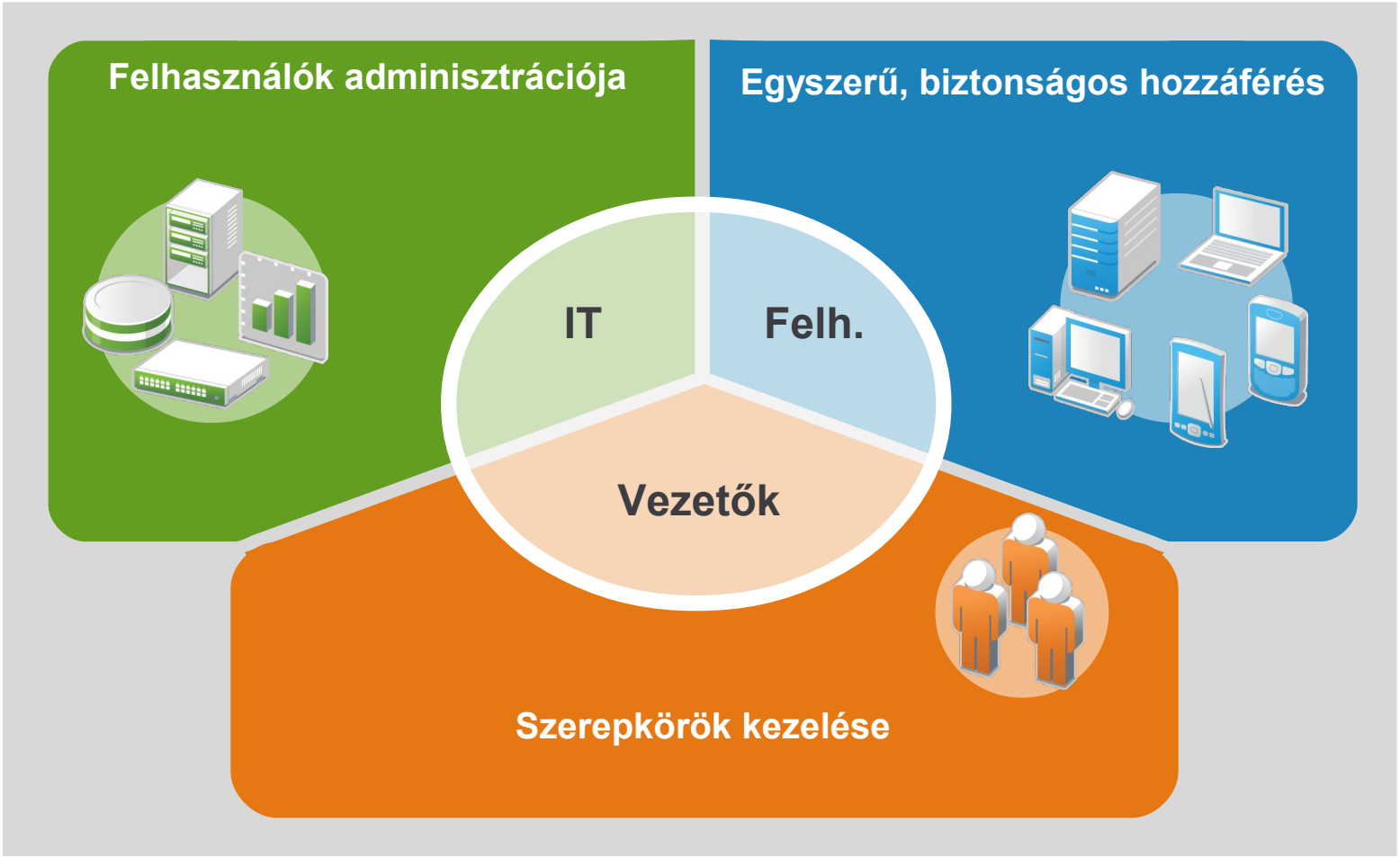
Hogyan lehet a jelszavakkal kapcsolatos problémákat csökkenteni?

Hogyan lehet kialakítani egy olyan környezetet, ahol mindenki csak a munkájához szükséges  minimális jogosultságokkal rendelkezik?

Hogyan lehet hatékonyan kezelni a rendszerhez kapcsolódó külső felhasználókat és partnereket?

Hogyan lehet a folyamatosan változó vonatkozó szabályoknak és előírásoknak precízen megfelelni?

# Identity és Access Management megoldások



# Miben segít egy IDM rendszer?

## Biztonság

- Jogosultságok visszavonása percek és nem napok alatt
- Jelszavak központosított kezelése
- Alkalmazottak csak ahhoz kapnak hozzáférést amihez feltétlenül szükségük van
- Megszünteti a duplikált nyilvántartásokat

## Megfelelőség

- Egyértelmű nyilvántartás arról, hogy ki mihez fér hozzá és a hozzáférést ki hagyta jóvá
- Historikus riportok
- Ütköző jogosultságok kimutatása
- Céges irányelvek egyszerű leképezése
- Azonnali dokumentációkészítés auditoroknak

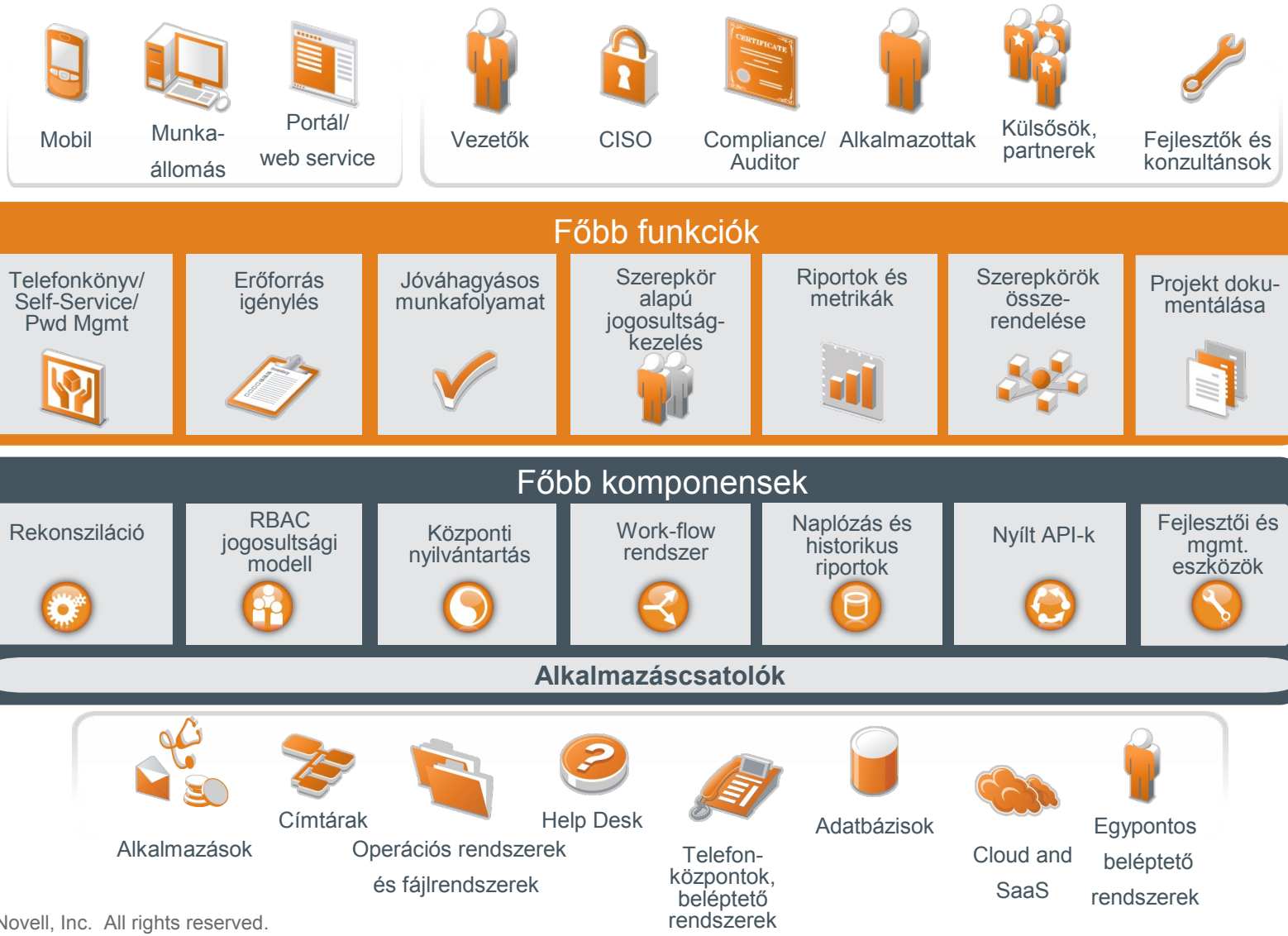
## Költségek

- Nagyban csökkenti a helpdesk hívások számát
- Munkafolyamatok elektronikus útra való terelése
- Új alkalmazások bevezetésének egyszerűsítése
- Gyors és költséghatékony implementáció

## Rugalmasság

- Új folyamatok napok alatt bevezethetőek
- A munkatárs felvételét követően a szükséges jogosultságok azonnal rendelkezésre állnak
- A felhasználók saját maguk igényelhetnek erőforrásokat
- Az üzleti döntések alakíthatják ki az IT szabályokat és nem fordítva

# Tipikus IDM architektúra logikai nézete



# Identity Manager működés közben

# IDM rendszer működés közben

# IDM projektek tipikus problémái

- Scope hibás meghatározása
- Szerepkörösítés megvalósítása, helyes módszer és a szerepkörösítés mértékének kijelölése
- Adattisztítás
- Éles indítás lépései
- Üzemeltetési szerepek meghatározása

# A projekt scope-ja

**Olyan scope-ot kell meghatározni:**

- Maximum 6-8 hónap alatt megvalósítható és a felhasználók széles rétege számára kézzelfogható eredményeket hoz
- Az architektúra és üzleti logika szempontjából lehetőség szerint teljes körű
- Az auditorok számára már elfogadható megoldást jelent
- Fenntartható és könnyen továbbfejleszthető környezetet alakít ki
- A legfontosabb IT rendszerekre koncentrál

# A projekt scope-ja

**Mivel lehet a scope-ot ésszerűen csökkenteni?**

- A legfontosabb alkalmazásokat és rendszereket on-line csatoljuk, a többit off-line rendszerként hagyjuk meg.

- Off-line rendszereknél automatikus ütemezett jogosultság-visszaellenőrzést valósítunk meg.

- A szerepkörök fogadásához szükséges struktúrákat felépítjük, de csak a szerepkörök legfelső szintjét töltjük fel tartalommal.

- Azon riportokat és kimutatásokat készítjük el amelyek feltétlenül szükségesek (pl. PSZÁF szempontból)

- Teljes körű adattisztítást csak az on-line rendszerekre végzünk.

# Szerepkörösítés

**Mi az a szerepkör?**

· A jogosultságok olyan csoportja, amely a tipikus felhasználó tevékenységek mentén szervezett. A szerepkör lehet alkalmazáson belüli és alkalmazásokon átívelő.

**Előnyei:**

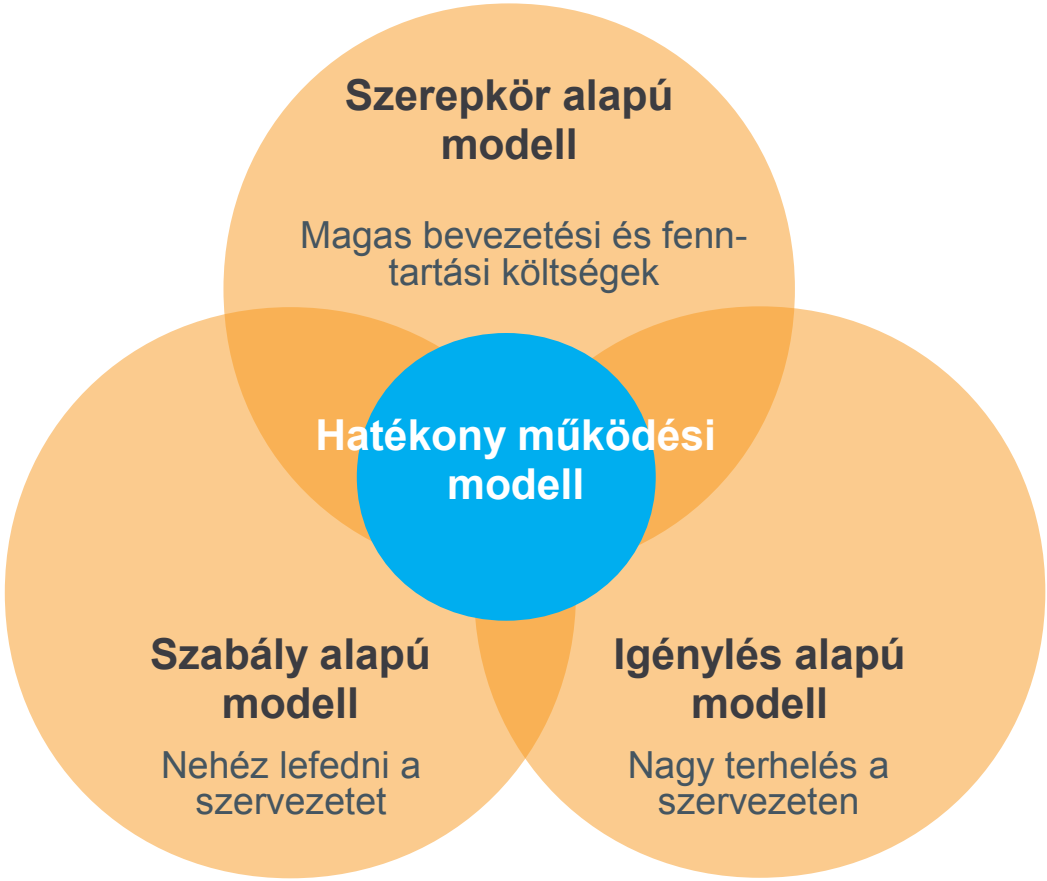
· Jogosultságok nagy részének beállítása automatikus.

· Tömegesen lehet jogosultságokat változtatni.

· Munkafolyamatok száma nagymértékben csökken.

· Felesleges jogosultságok könnyebben kiszűrhetőek.

# Optimális helyzet



# Szerepkörök kialakításának módszerei

**Top Down – felhasználók oldaláról indított**
A szerepköröket a felhasználók attribútumai alapján próbáljuk meg kialakítani. Különböző szerepkörök csoportokat kaphatunk különböző attribútumok alapján vizsgálódva.

**Top Down – jogosultságok oldaláról indított**
A felhasználókat keressük meg a jogosultsági csoportokhoz. Ez a módszer azt feltételezi, hogy jól ismert a jogosultságok kiosztásának rendje.

**Bottom Up**
Mintákat keresünk a kiosztott jogosultságokban. Akkor alkalmazandó, ha sem a felhasználói csoportokat, sem a jogosultságok kiosztásának módját nem ismerjük. Kis létszámú szervezeteknél alkalmazható.

**Interjúk**
A szakmai területekkel egyeztetve találjuk meg a minimálisan szükséges jogosultsági csoportokat.

# Tipikus szerepkör kezelés

1 2 3

Az IDM rendszer ősfeltöltése a lehetséges szerepkörökkel

## Szerepkör bányászat

Kigyűjti, hogy milyen jogosultságokkal rendelkeznek a felhasználók.

## Szerepkör modellezés

A gyűjtött adatok alapján tervezi, modellezi a szerep-köröket

## Hozzáférés ellenőrzés

A vezetők ellenőriz-hetik, hogy kinek, milyen joga van

A hozzáférés ellenőrzés eredményeképpen változó környezet újratervezést vonhat maga után

# Tipikus szerepkör kezelés

1 2 3

Jogosultságok beállítása automatikusan a kiosztott szerepkörök alapján

## Szerepkörök felhasználása

Az IDM rendszer felhasználja a szerep-köröket alapadatként.

## Automatikus beállítás

A jogosultságok be-állítása automatikus, ezzel csökken a hibák száma és emelkedik a biztonság szintje.

# Tipikus szerepkör kezelés

1 2 **3**

A felhasználói tevékenységek folyamatos ellenőrzése: SIEM rendszer

**Vizsgálat**

A jogosultságok használatának ellenőrzése.

**Elhárítás**

Kiosztott jogosultságok módosítása az IDM-ben ha szükséges.

**Újratervezés**

A szerepkörök újra-tervezése, hogy minél kevesebb felesleges jog legyen kiosztva.

Ez a folyamat folytonos, nem csak egy auditot követően történik meg

# Adattisztítás fontossága

## Adathibák

- Hibás adat
- Rosszul formázott adat
- Hiányos adat
- Duplikátumok
- Hiányzó adat
- Nem egyező adat
- Séma nem tisztázott
- Ősfeltöltési nehézségek
- Asszociációk felépítése

## Problémák

- Rossz döntések
- Folyamatok hibás definiálása
- Biztonsági rések
- Megfelelőség hiánya
- Nem gazdaságos megoldás
- Magas erőforrásigény
- Információvesztés

# Adattisztítási folyamat


Adatok online és offline begyűjtése

Az adatok állapotának meghatározása mintaillesztéssel, statisztikai módszerekkel

Adatok tisztítása (manuális, tömeges, automatikus, szkript alapú)

Egyediség vizsgálat

Adatforrások összegzése

Tisztított adatok visszatöltése

Az adatok folyamatos monitorozása (pl. reconciliation)

# IDM rendszer élesbe állítása

**Fontos lépések a rendszer éles indulásának időszakában:**

- Kulcsfelhasználók oktatása
- On-line tananyag létrehozása
- Üzemeltetők és HelpDesk oktatása
- Szabályzatok módosítása
- Hagyományos jogosultságigénylő folyamatok blokkolása
- Mentés, monitorozás beállítása
- Éles indulást követő kiemelt támogatás biztosítása
- Üzemeltetési szerepek meghatározása

# Üzemeltetési szerepek

- Hagyományos (OS, címtár, adatbázis, mentések stb.)
- Szerepkörök és SOD szabályok folyamatos ellenőrzése
- Munkafolyamatok módosítása, a változó környezethez igazítása
- Jóváhagyói csoportok, kiemelt IDM szerepek adminisztrációja

# Riportok, kimutatások

**PSZÁF elvárások:**

- kinek milyen jogosultsága van, illetve volt
- adott jogosultsággal ki rendelkezik, illetve rendelkezett
- ki hagyta jóvá az adott jogosultságot
- technikai felhasználók jogosultságai
- SOD mátrix
- ütköző jogosultságok

# További tipikus riportkövetelmények

- Előkészített riportok, amelyek bővíthetőek, testre szabhatóak
- Compliance (megfelelőségi) riportok
- Attestation (újra hitelesítési) riportok
- Segregation of Duties (összeférhetetlenségi) riportok
- Hisztorikus adatkezelés adatelem szinten
- Csomóponti és átfutási idő statisztikák
- Munkafolyamatokkal kapcsolatos egyéb riportok


Kérdések?


Novell®