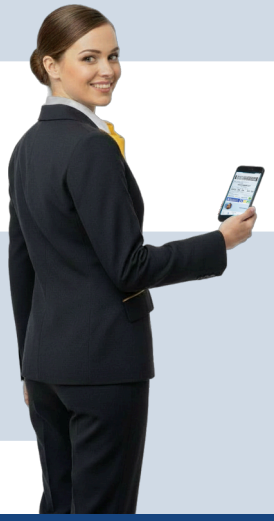
MÁV SZOLGÁLTATÓ KÖZPONT ZRT.

INFORMÁCIÓBIZTONSÁGI TUDATOSÍTÁS

# Amit nem látunk, azt nem védhetjük meg

## Shadow IT és Shadow AI a mindennapi munkában

Egy gyors fájlmegosztás, egy praktikus online segédprogram vagy egy AI-asszisztens elsőre ártalmatlannak tűnik. Ha azonban az informatikai és az információbiztonsági terület nem tud róla, a szervezet adatai olyan helyre kerülhetnek, amelyet senki sem felügyel.



> **Amit a szervezet nem ismer, annak a kockázatát sem tudja megfelelően kezelni.**

1 · Mi a Shadow IT? 2 · Kockázatok 3 · Shadow AI 4 · Mit tehetünk?

# 1 Mi a Shadow IT?

Shadow IT-nak nevezzük azokat az eszközöket, alkalmazásokat és szolgáltatásokat, amelyeket munkavégzésre használunk, de az **informatikai vagy az információbiztonsági terület nem tud róluk**. Így a szervezet olyan rendszerekkel és adatkezelési folyamatokkal kerül kapcsolatba, amelyeket nem tud felügyelni.

A probléma nem az, hogy új eszközöket veszünk igénybe, hanem az, hogy ezek a megszokott **biztonsági, hozzáférés-kezelési, adatvédelmi és beszállítói kontrollokon kívül** működhetnek. A Shadow IT legújabb formája a Shadow AI.

## Hogyan alakul ki?

**01 Konkrét probléma**
Túl nagy a fájl, nehézkes a hivatalos rendszer, hiányzik egy eszköz.

**02 Gyors megoldás**
Felhőtárhely, online segédprogram vagy új kommunikációs alkalmazás.

**03 Rendszeressé válik**
Ha beválik, újra és újra használjuk – egy regisztráció elég hozzá.

**04 Folyamat épül rá**
Egy teljes munkafolyamat függ egy nem felügyelt szolgáltatástól.



A Shadow IT jellemzően nem tudatos szabályszegéssel kezdődik. Gyakran arra utal, hogy rés keletkezett a felhasználói igények és a hivatalosan biztosított informatikai lehetőségek között.

**Közös jellemzőjük:** úgy kerülnek be a munkavégzésbe, hogy adatkezelési és biztonsági feltételeik nem mentek végig a szervezet szokásos ellenőrzési folyamatain.

## Tipikus megjelenési formák

- Nem engedélyezett felhőtárhely
- Külső fájlmegosztó
- Online segédprogram
- Kommunikációs, közösségi felület
- Böngészőbővítmény
- Kisebb SaaS-szolgáltatás
- Saját eszköz munkacélra
- **Nem jóváhagyott AI-szolgáltatás**

# 2 Milyen kockázatot jelent?

A Shadow IT legnagyobb kockázata, hogy a szervezet olyan szolgáltatásokat használhat, amelyek **kívül esnek a megszokott biztonsági és üzemeltetési kontrollokon**.

### Ismeretlen adatkezelés

Nem tudjuk, milyen adatok kerülnek a szolgáltatásba, hol és meddig tárolják, ki fér hozzájuk, és hogyan törölhetők.

### Kicsúszó hozzáférések

Az önállóan létrehozott külső fiók egy munkatárs távozása után is aktív maradhat – a központi felügyelet nem látja.

### Vakfolt a naplózásban

Az ismeretlen rendszerek eseményei kimaradnak a szervezeti naplózásból, ami megnehezíti egy incidens észlelését és kivizsgálását.

### Üzletmenet-függőség

Ha egy munkafolyamat ilyen szolgáltatásra épül, annak kiesése az üzletmenetet is érintheti.

### Beszállítói kockázat

Adatokat vagy folyamatokat bízunk olyan külső szolgáltatóra, amelyet a szervezet előzetesen nem értékelt.

### Megfelelőségi kockázat

A nem ismert megoldások adatvédelmi és megfelelőségi kockázatot hoznak létre, miközben a kezelésükhöz szükséges rálátás hiányzik.

A KÖZÖS NEVEZŐ

**Ha a szervezet nem tud egy szolgáltatás használatáról, annak kockázatait sem tudja felmérni és kezelni.**

# 3 Shadow AI – a Shadow IT új arca

Shadow AI-ról beszélünk, amikor munkavégzésre olyan **mesterségesintelligencia-szolgáltatást** használunk, amelyet a szervezet nem hagyott jóvá, vagy biztonsági szempontból nem vizsgált. Szolgáltatásonként eltérhet, hogy a bevitt adatokat **meddig őrzik meg, mire használják fel, és kik férhetnek hozzájuk**.

### ⚠ A kockázat akkor jelentkezik, ha átadunk...

- Belső dokumentumot
- Forráskódot
- Személyes adatot
- Egyéb érzékeny információt



## Miért nehéz észrevenni?

Az AI egyre gyakrabban beépül a mindennapi eszközökbe, így nem mindig egyértelmű, mikor kerül adat külső szolgáltatóhoz.

- **Böngészők**
- **Irodai alkalmazások**
- **Levelezőrendszerek**
- **Fejlesztői környezetek**

## Több, mint adatszivárgás

A Shadow AI kockázatai ezeket a területeket is érintik:

- Hozzáférés-kezelés
- Beszállítói kockázat
- Megfelelőség
- Incidenskezelés
- Hibás vagy pontatlan AI-tartalom felhasználása

**Nem az a kérdés, használjuk-e az AI-t, hanem hogy a szervezet tudja-e: milyen szolgáltatást, milyen adatokkal és milyen feltételek mellett használunk.**

# 4 Mit tehetünk?

A Shadow IT kezelésének első lépése nem a tiltás, hanem a **láthatóság**. A cél nem minden új technológia kizárása, hanem a ténylegesen használt informatikai környezet feletti rálátás és ellenőrzés megőrzése.

## Munkatársként

- Munkavégzéshez a jóváhagyott eszközöket és szolgáltatásokat használjuk.
- Belső dokumentumot, forráskódot, személyes adatot nem adunk át nem jóváhagyott külső vagy AI-szolgáltatásnak.
- Új szolgáltatás bevonása előtt előzetesen egyeztetünk.
- Ha a hivatalos eszköz nem elég, jelezzük az igényt – nem kerülőúton oldjuk meg.
- Ha már használunk nem jóváhagyott megoldást, jelezzük: a cél a rálátás, nem a tiltás.

## A szervezet oldalán



### Láthatóság
Megismerni, milyen külső szolgáltatásokat és eszközöket használunk, és milyen adatok kerülnek beléjük.

### Az okok megértése
Ha a hivatalos eszköz nehézkes vagy hiányzik egy funkció, kerülőutak alakulnak ki.

### Szabályok és alternatívák
Egyértelmű szabályok, jól használható engedélyezett eszközök, egyszerű jóváhagyási folyamat.

### Technikai kontrollok
Indokolt esetben naplózás, hozzáférés-korlátozás vagy végponti felügyelet.

**Kérdés, igény vagy bizonytalanság esetén** forduljunk az informatikai, információbiztonsági területhez (ITCVB, HelpDesk) vagy az Információbiztonsági Felelőshöz – még a szolgáltatás használatba vétele előtt.

Forrás: Nemzeti Kiberbiztonsági Intézet – IT-biztonsági trendek: „Amit nem látunk, azt nem védjük – Shadow IT és Shadow AI”.