



ENTERPRISE  
GROUP



BYOD

Bring Your Own Device

Approved Partner  
Siemens Enterprise  
Communications

SIEMENS



## BYOD – Bring Your Own Device vagyis „Hozd magaddal a saját eszközöd”

Magyarországon a táblagépek és az okostelefonok gyors terjedésével és azzal, hogy hazánkban is számos üzleti célú, mobil eszközre optimalizált alkalmazás válik elérhetővé, egyre több vállalat ismeri fel, hosszabb távon elkerülhetetlen, hogy alkalmazottaik a saját gépeiken is dolgozzanak.

A hálózatbiztonság egyik legfontosabb trendje ezért a következő években egyértelműen a Bring Your Own Device (BYOD), vagyis a „Hozd a saját eszközöd” lesz, hiszen a felhasználók a közeljövőben minden eddignél nagyobb számban viszik majd magukkal mobil eszközeiket a munkahelyekre és használják azokat egyre gyakrabban mindennapi munkájuk során. A munkahelyek többségénél már most is lehetséges a vállalati erőforrásokhoz történő csatlakozás, azonban a BYOD rendszer lehetővé teszi a forgalom szabályozása mellett a naplózást, valamint azt, hogy ne csak a hálózati csatlakozás legyen biztosított, hanem a csatlakozott eszközön a munkavégzés biztonságos és szabályozott módon történhessen meg.

### BYOD tendenciák Magyarországon\*

- Az alkalmazottak 60%-a rendelkezik olyan mobil eszközzel, amellyel csatlakozni tud a céges hálózathoz, és el tud érni céges adatokat és alkalmazásokat.
- A vállalatok több mint felénél (53%) engedélyezik a céges hálózathoz való hozzáférést a munkavállaló saját tulajdonú készülékével.
- A felmérésben résztvevők 43%-a válaszolta, hogy a céges hálózatba csak biztonságos kapcsolaton keresztül tud belépni, 24% bármilyen más kapcsolaton keresztül is tud csatlakozni.
- A kutatás tanulsága szerint a távoli hozzáférések során az e-mail alkalmazásokat használják a legnagyobb mértékben (65,5%), ezt az irodai alkalmazások, és a naptár használata követi.
- A globális trendekhez hasonlóan csak a hazai vállalatok 56 %-nál van valamilyen szabályozás a mobil eszközök céges hálózathoz való hozzáférésehez, és mindössze 8% tervezi, hogy hat hónapon belül kialakítja szabályrendszerét a trend kezelésére. A válaszadók 19%-nál nincs semmiféle szabályozás, 18% pedig nem tudja, hogy létezik-e ilyen a vállalatnál.

\*Forrás: Cisco IBSG Horizons Study

# A BYOD széleskörű előnyöket nyújt

A BYOD-nak számtalan előnye van, így a vállalatoknak érdemes kiaknázni a benne rejlő lehetőségeket. Az óvatosság és a szakértelem kiemelten fontos, mert a szükséges megfontolások nélkül könnyen teherré válhat, megvalósítása pedig törvényi- vagy egyéb vállalati felelősségbe ütközhet.

## Csökkenő költségek

A BYOD komoly költségcsökkentést tesz lehetővé a cégek számára, hiszen ha az alkalmazottak saját gépükön dolgoznak, a vállalat megspórolhatja ezen eszközök beszerzését és üzemeltetését.

## Hatékonyabb munkavégzés, nagyobb rugalmasság

Azzal, hogy lehetővé válik a vállalati hálózat távoli elérése bármely eszközről, az alkalmazottak képesek hozzáférni az információkhoz, kommunikálni és együttműködni saját munkatársaikkal.

## Javuló munkavállalói elkötelezettség

Kitűnő motivációs eszköz, amely ráadásul ingyen van (leszámítva a céges biztonságra számított költségeket.)

A BYOD egy olyan komplex rendszer, amely az alábbi funkciókat teljesíti:

- csatlakozási felület biztosítása a hálózathoz (vezetékes hálózat, WiFi),
- csatlakozó eszközök azonosítása (gyártó, szoftververzió),
- mobil eszközön futtatott szoftverek felmérése (például víruskereső, tűzfal),
- nem megfelelő szoftverek használata esetén keretrendszer nyújtása a telepítéshez, frissítéshez.







## A kulcs a megfelelő szabályozás

A BYOD biztonságos használatához alapos szabályozás, megfelelő vállalati eszközök és felhasználói ismeretek szükségesek, ezek hiányában ez a feladat komoly biztonsági kihívást jelent a vállalatok számára. Melyek a legfontosabbak?

### **Az elérhető adatok körének korlátozása**

Ahhoz, hogy a BYOD rendszer támogatásához szükséges IT erőforrások tervezhetőek legyenek, kellő körültekintéssel kell megválasztani azon alkalmazásokat, amelyeket elérhetővé teszünk. Csak azon alkalmazásokat javasolt mobil eszközökön is futtatni, amelyek esetén fontos a mobilitás.

### **Vállalati adatok biztonságának garantálása**

A mobil eszközök sajátossága, hogy azok könnyebben sérülhetnek, ellophatják vagy elveszíthetik őket, így a céges adatok illetéktelen kezekbe kerülhetnek. A nem csak munkára használt telefonokkal és tabletekkel emellett olyan kommunikációs formákra is lehetőség nyílik, amelyek során érzékeny vállalati adatok kerülhetnek ki a cégtől. Erre ma már számos olyan felügyeleti megoldás létezik, amellyel a telefonok és tabletek – a céges PC-khez hasonlóan – távolról is kezelhetők és tiltathatók. Az ún. Mobile Device Management (MDM) megoldások képesek nem csak a blokkolást, de a teljes körű hozzáférést is lehetővé tenni, így az informatikai szakemberek kijelölhetik és elmenthetik a mobil eszközök vállalati tartalmát.

### **A privát és a vállalati adatok biztonságos szétválasztása**

A BYOD rendszerek lehetővé teszik a privát és a vállalati adatok teljes körű és biztonságos szétválasztását. Ezzel megoldható e trend egyik legfontosabb kérdése: az adminisztrátorok megvédhetik a személyes és vállalati tartalmakat a készülék érintése nélkül. Ehhez célszerű egy megállapodást aláírni az alkalmazottakkal, hogy a vállalattól való távozás esetén – a személyes adatok érintése nélkül – az összes bizalmas vállalati adat törlésre kerül telefonjaikról, illetve táblagépeikről.

## Házirend és jogosultságok

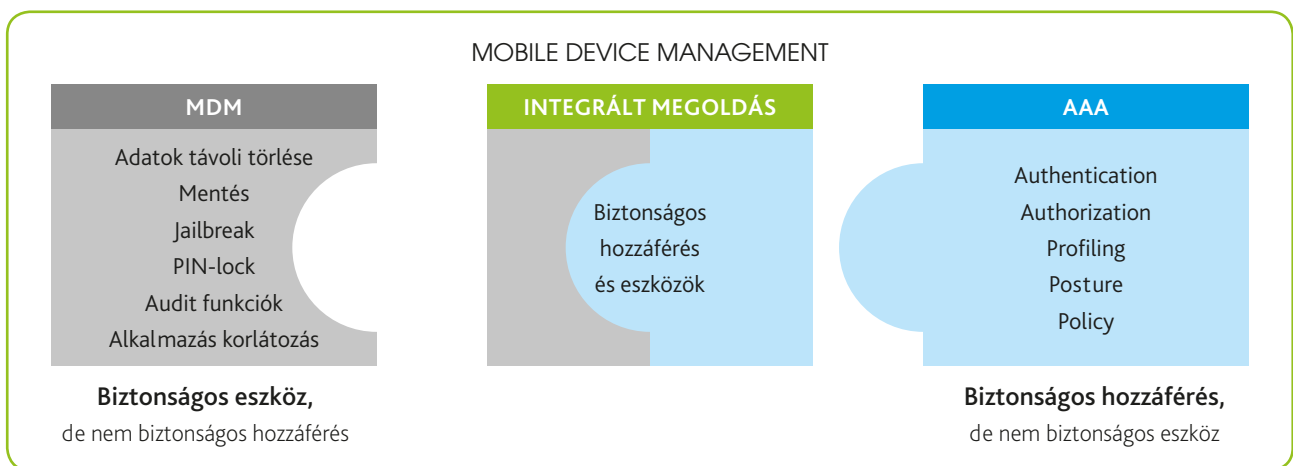
A biztonságos és helyes eszközhasználat alapja, hogy az alkalmazottak ismerjék lehetőségeiket és kötelességeiket. Ennek módja lehet a belső szabályozás, amely rögzíti, mely pozíciók esetén engedélyezett a saját eszközön történő munkavégzés és ehhez milyen biztonsági előírásokat kötelező betartani (például központi jelszó házirend).

## Vállalati alkalmazások mobilizálása

A dolgozói eszközökre folyamatosan számos üzleti alkalmazás jelenik meg az irodai megoldásoktól az üzletiintelligencia-klienseken át az ügyfél-nyilvántartási rendszerekig, vagyis ezek az eszközök remekül használhatók akár rendszeres munkavégzésre is. Ha egy vállalat a megfelelő jogosultságokat figyelembe véve teszi elérhetővé ezeket a programokat, alkalmazottai saját mobil eszközeikről is teljes értékű munkát végezhetnek.

## Használható eszközök körének szabályozása

A BYOD bevezetése során javasolt meghatározni az alkalmazások által megkövetelt hardver és szoftverigényeket, az ezeknek megfelelő készülékek köréből pedig a felhasználók szabadon választhatnak.



## BYOD szolgáltatásunk

Teljes körű szolgáltatást nyújtunk a tanácsadástól a megvalósításon át egészen az üzemeltetésig.

### Tanácsadás:

Amennyiben Önnél még nincs BYOD, tanácsadás keretében Önnel közösen áttekintjük az igényeiket, és javaslatot teszünk a rendszerre vonatkozóan.

### Ha már rendelkezik BYOD rendszerrel:

Áttekintjük a meglévő rendszerét, felmérjük a kockázatokat, javaslatot teszünk a rendszer optimalizálására.

### Megvalósítás és üzemeltetés:

Igény esetén megtervezzük és megvalósítjuk Önnek a BYOD rendszert, és közreműködünk az üzemeltetésben.

Ha Ön is szeretné, hogy cége hatékonyabban működjön, a munkatársak távolléte ne akadályozza a folyamatok működését, és biztonságban szeretné tudni cége érzékeny adatait, akkor a BYOD rendszer megoldást jelent az Ön számára. Munkatársai közül már biztosan van, aki saját eszközt használ, a cégvezetés arról dönthet, hogy ezt milyen szabályozások mentén, mennyire biztonságosan tegyék.

### Működünk együtt, keresse szakértőinket!

 **ICT**  
ÜZLETÁG

 **PLM**  
ÜZLETÁG

 **SOFTWARE**  
ÜZLETÁG

 **CONSULTING**  
ÜZLETÁG

## KAPCSOLAT

---

H-1143, Budapest, Gizella út 51-57.

T: +36 1 471 2400

F: +36 1 471 2402

e-mail: [info@enterprisegroup.hu](mailto:info@enterprisegroup.hu)

[www.enterprisegroup.hu](http://www.enterprisegroup.hu)



**ENTERPRISE**  
GROUP