

Cloud Security

Homo mensura

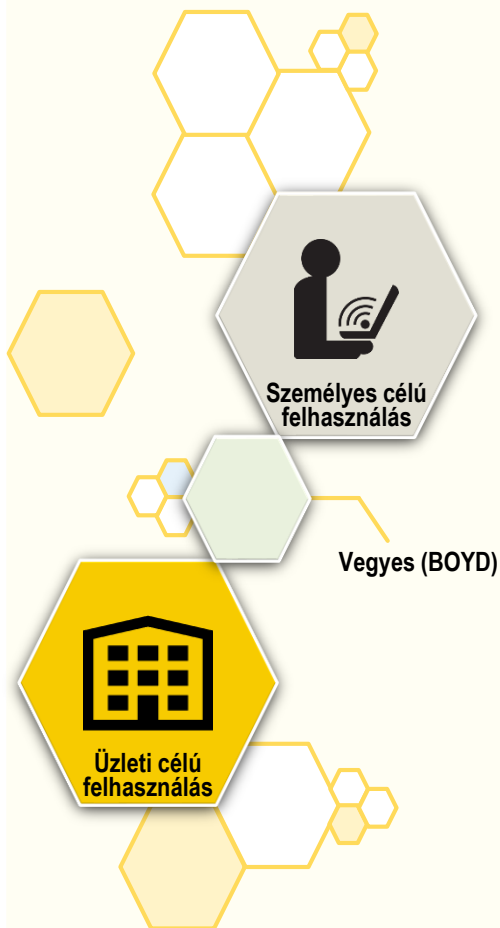
2018. november

Sallai Gyorgy



The better the question. The better the answer. The better the world works.

Adatkezelés számokban



Felhasználókra vonatkozó statisztikák

**9,9
M**



KSH-adat szerint 2016-ban Magyarország lakossága meghaladta a 9,9 millió főt

KSH-adat szerint 2016-ban Magyarország 7,2 millió aktív internet-felhasználót regisztráltak



**7,2
M**

**4,9
M**



Az Internet World Stats adatai szerint a hazai facebook-felhasználók száma 2016-ban elérte a 4,9 milliót

Adata tárolásra és- forgalomra vonatkozó statisztikák

**41
PB**

(peta: 10^{15})



Az IDC adata szerint míg a szervereladások hazánkban csökkentek, addig a tároló piac folyamatos növekedése mellett 2016-os eladás 41 petabyte

A KSH adatai szerint 2016-ban a mobilhálózati adatforgalom elérte a 29 petabyte-ot



**29
PB**

**1,1
EB**

(exa: 10^{18})



A CISCO 2016-os VNI (Visual Network Index) előrejelzése szerint az IP-forgalom éves szinten meghaladja az 1 exabyte-ot.

Felhőszolgáltatások elfogadottsága



Elköteleződés a felhő szolgáltatások iránt

86%



Általánosan megállapítható, hogy a társaságok 86%-a az IT költségvetésük egy részét felhőszolgáltatásokra költi,

20%



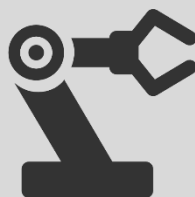
Átlagosan a társaságok IT költségvetésük 20%-át teszi ki a felhőszolgáltatások. Ezt az értéket az 5k alkalmazottal rendelkező társaságok 36%-a éri el, míg az 5k alatti foglalkoztatók 49%-a.

41%



A társaságok 41%-a óvatosan fordul a felhőszolgáltatások felé, mert nem tartja biztonságosnak. Ez az arány az USA-ben 37%, míg az Európai régióban 52%. Annak ellenére, hogy a támadások nagyrésze az USA-t éri

Symantec IT bizalmi index



51%

Az 50 főnél nagyobb vállalkozások az IT stratégiai területének tartják. 51% házon belül tartaná az infokommunikációs megoldásokat és fejlesztéseket.

36%



Az 50 fő alatti vállalkozások kevesebb figyelmet szentelnek az IT-megoldásokra és csupán 36% gondolja, hogy az IT-infrastruktúrát házon belül kell tartani.

Felhőszolgáltatások felhasználását bemutató adatok



Felhőben tárolt vállalati adatok

#1

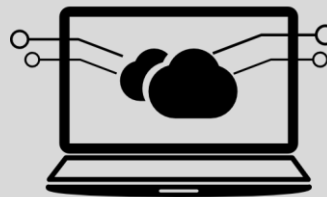


Email a leggyakrabban kiszervezett adat

#2



Sales-Marketing adatok



#3



Szellemi tulajdon

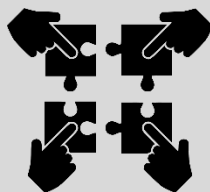
#4



Ügyféladat, ami a legjobban támadott adattípus

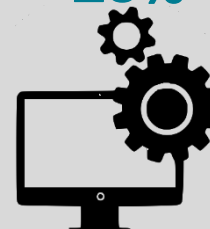
Felhő alkalmazások népszerűsége

56%



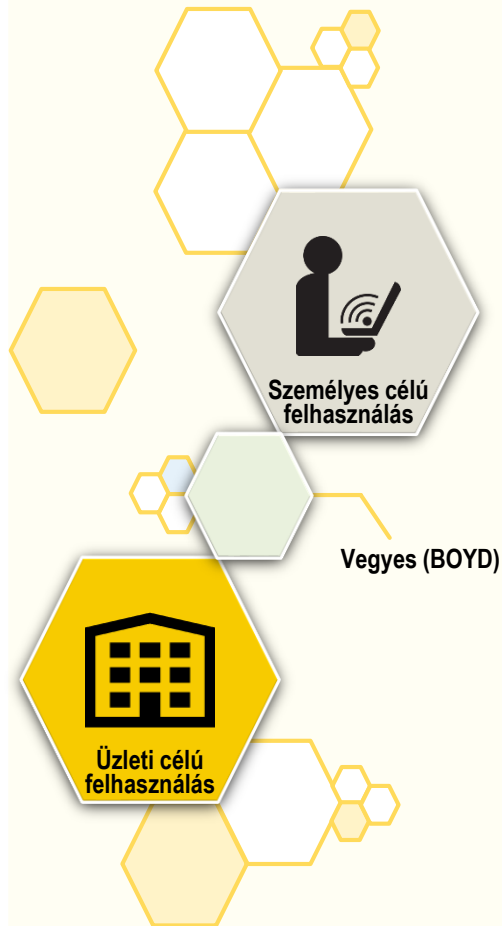
Az alkalmazások 56%-a kollaborációt és a sales marketing tevékenységet elősegítő megoldások. Ezt követi csak a produktivitás támogató megoldások.

26%



Az alkalmazások kevesebb mint 26%-a ami az IT üzemeltetést segíti. Ebből a tesztelést 24%-nyi alkalmazás támogatja, az adat mentést, helyreállítást 23%.

Visszatartó tényezők a felhőszolgáltatással szemben

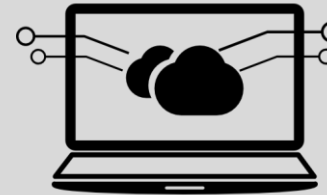


A felhőszolgáltatás előnyei és hiányosságai

51%

A megkérdezettek 51%-a jelentős előnyöket lát a felhő szolgáltatások alkalmazásában

- #1 Flexibilitás
- #2 Rendelkezésre állás
- #3 Költségcsökkentés



22%

A kutatásban résztvevők 22%-a szerint a biztonság és 9%-a szerint a törvényi megfelelés az egyedüli hátránya a felhőszolgáltatásoknak.

Biztonsági megfontolások

90%



A szervezetek 90%-ának komoly aggályai vannak a publikus felhőszolgáltatásokkal. Jelenleg a biztonság a legnagyobb gátja a felhő alapú működés terjedésének.

- #1 Általános biztonsági aggályok
- #2 Adatvesztés és adat szivárgás
- #3 Kontrollvesztés
- #4 Törvényi megfelelés
- #5 Integrációs problémák a meglévő IT-vel

Publikus felhőszolgáltatás Biztonsági fenyegetései



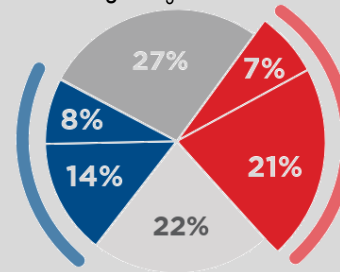
Publikus felhő biztonsági rései

22%

A megkérdezettek 22%-a szerint a biztonsági problémák a publikus felhőben alacsonyabbak, mint az on-premis megoldásoknál

- Szignifikánsan kisebb (8%)
- Valamelyest kisebb (14%)

A társaságok $\frac{1}{3}$ elszenvedett



biztonsági incidenst a felhőben

28%

A megkérdezettek 28%-a szerint a biztonsági problémák a publikus felhőben magasabbak, mint az on-premis megoldásoknál

- Szignifikánsan nagyobb (8%)
- Valamelyest nagyobb (14%)

Biztonsági megfontolások

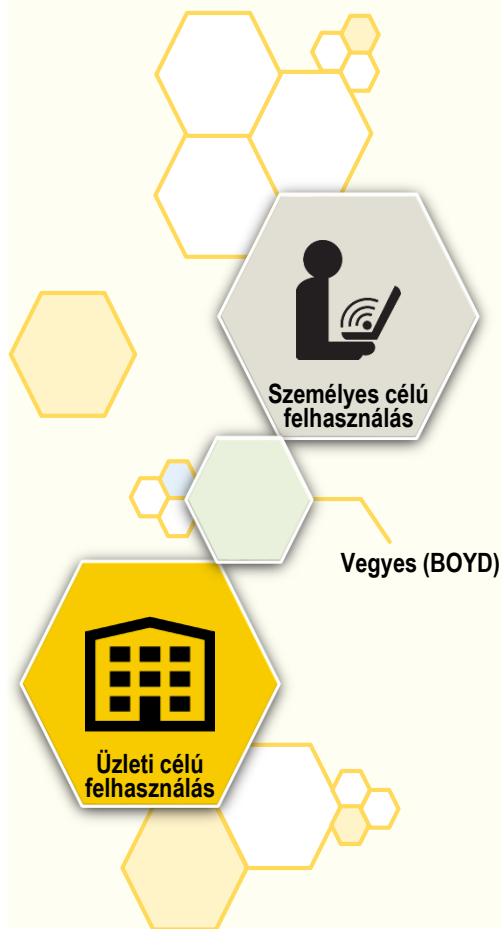


77%

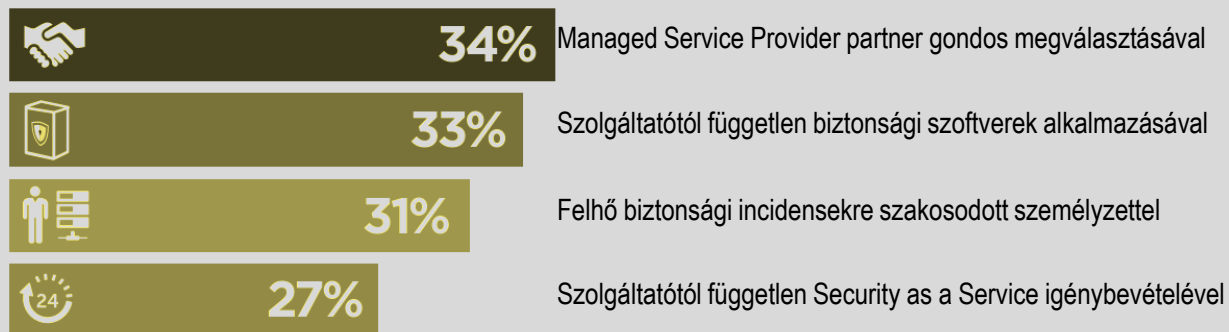
A célzott adatszerzésre irányuló támadások 77%-a profitvezérelt.

- #1 Jogosulatlan hozzáférés
- #2 Felhasználói azonosítók eltulajdonítása
- #3 Rosszindulatú belső felhasználó
- #4 Nem biztonságos interfész (API)
- #5 Szolgáltatásmegtagadási támadások (DOS)

Publikus felhőszolgáltatás Biztonsági fenyegetései



Felhőbe költözők hogyan kezelik a biztonsági igényeiket



Biztonság érzet növelése publikus felhő környezetben

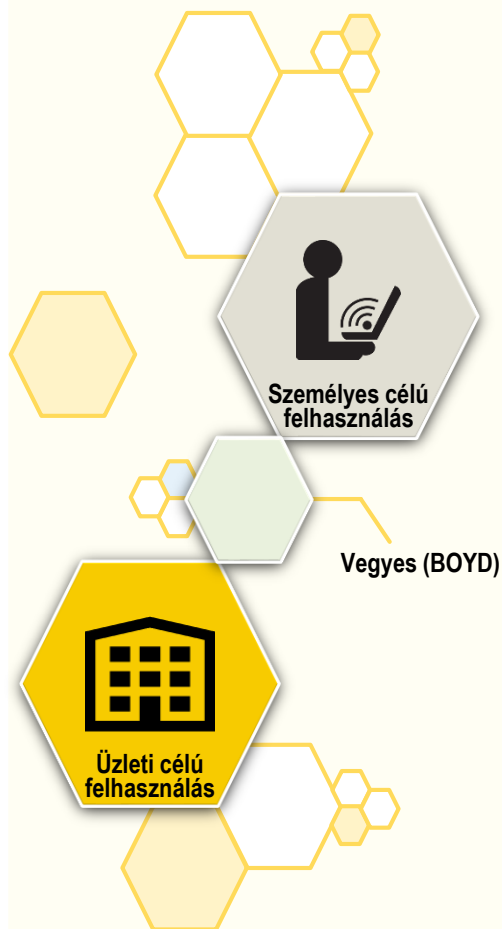
68%



A válaszadók 68%-a szerint a határvédelem nem kielégítő válasz felhő infrastruktúra védelmére. Az összetett támadások sikerei indokolják a további védelmi rétegek szükségességét.

- #1 Biztonsági policy kialakítás és kikényszerítése
- #2 Auditálhatóság megteremtése
- #3 Biztonsági kontrollok illesztése (cloud/on-premis)
- #4 Izolálható virtuális környezetek
- #5 Összehasonlítható biztonság a felhőszolgáltatóknál

Publikus felhőszolgáltatás kockázatai



Operációs kockázatok



Privilegizált felhasználók

Milyen kontrollok garantálják, hogy az adataimhoz ne férjen hozzá a szolgáltató



Helyreállítás

Mi történik az adataimmal katasztrófa esetén. Máshova kerül? Milyen gyorsan férhetek hozzá a helyreállított szolgáltatáshoz



Adatok lokációja

Hol tárolódik az adat, kikerül határon vagy EU-n kívülre? Lehet ezt befolyásolnia felhasználóként? Kié az adat ha már a felhőben van?



Adatok elkülönítése

Hogyan demonstrálja a szolgáltató, hogy más felhasználó nem láthatja az adataimat. Milyen titkosítást alkalmaz

Törvényi megfelelési kockázatok



Törvényi megfelelés

Hogyan lehet megfelelni a törvényi előírásoknak. A szolgáltatót auditálhatja a hatóság?



Nyomozati támogatás

Nyomozati esemény során ki tudom szolgálni a nyomozóhatóságot?



Hosszú távú életképesség

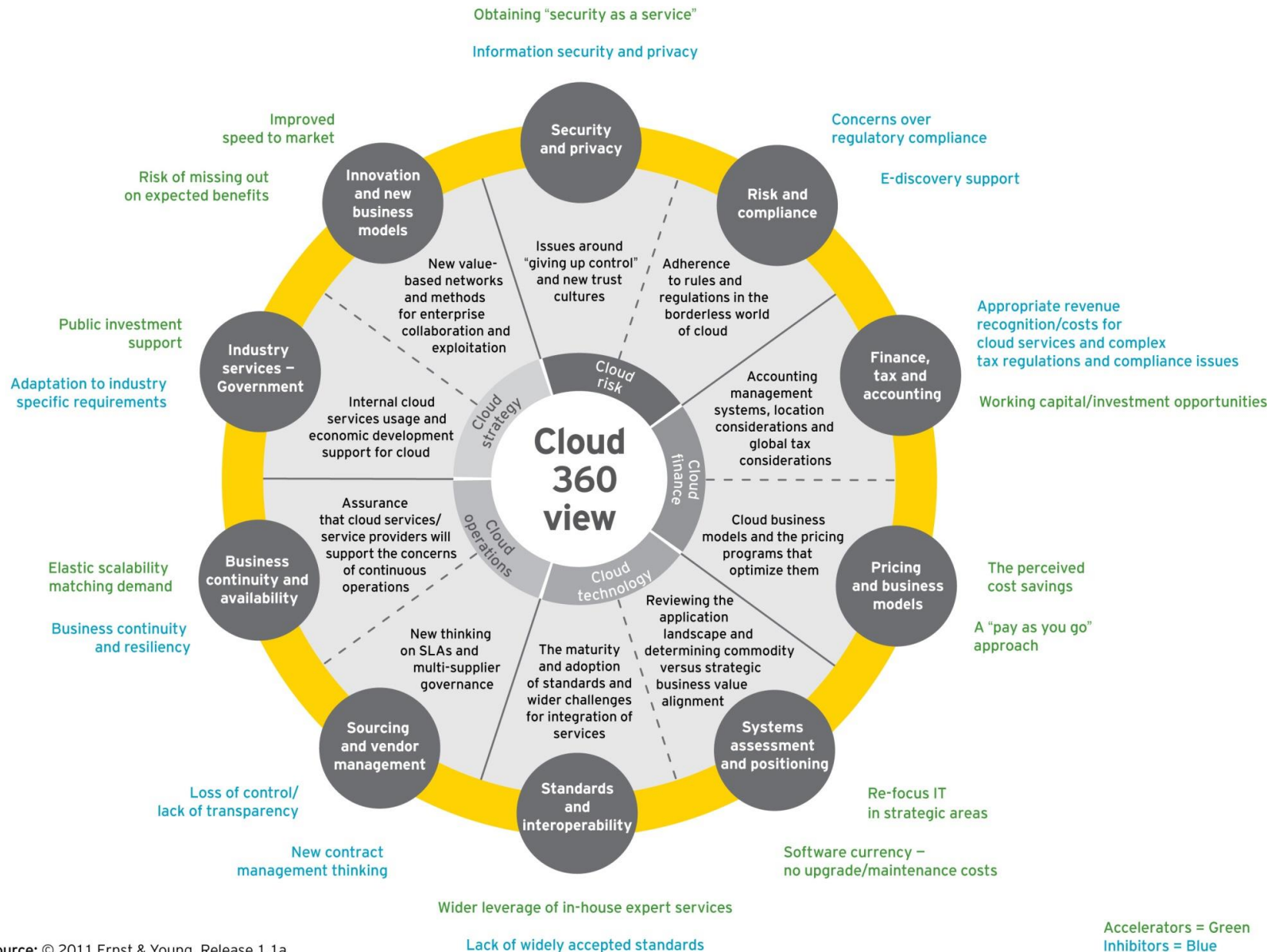
Hosszútávon mi történik az adataimmal. Ha a szolgáltató csődbe megy vagy felszámolják, hogyan kapom vissza az adataimat?



Adatszolgáltatás

Ha a bűnüldöző hatóság kikéri az adataimat a szolgáltatónak kötelessége-e értesítenie. Mi van ha tiltják a hatóságok?

Cloud 360° view





Gyorgy.Sallai@hu.ey.com

