

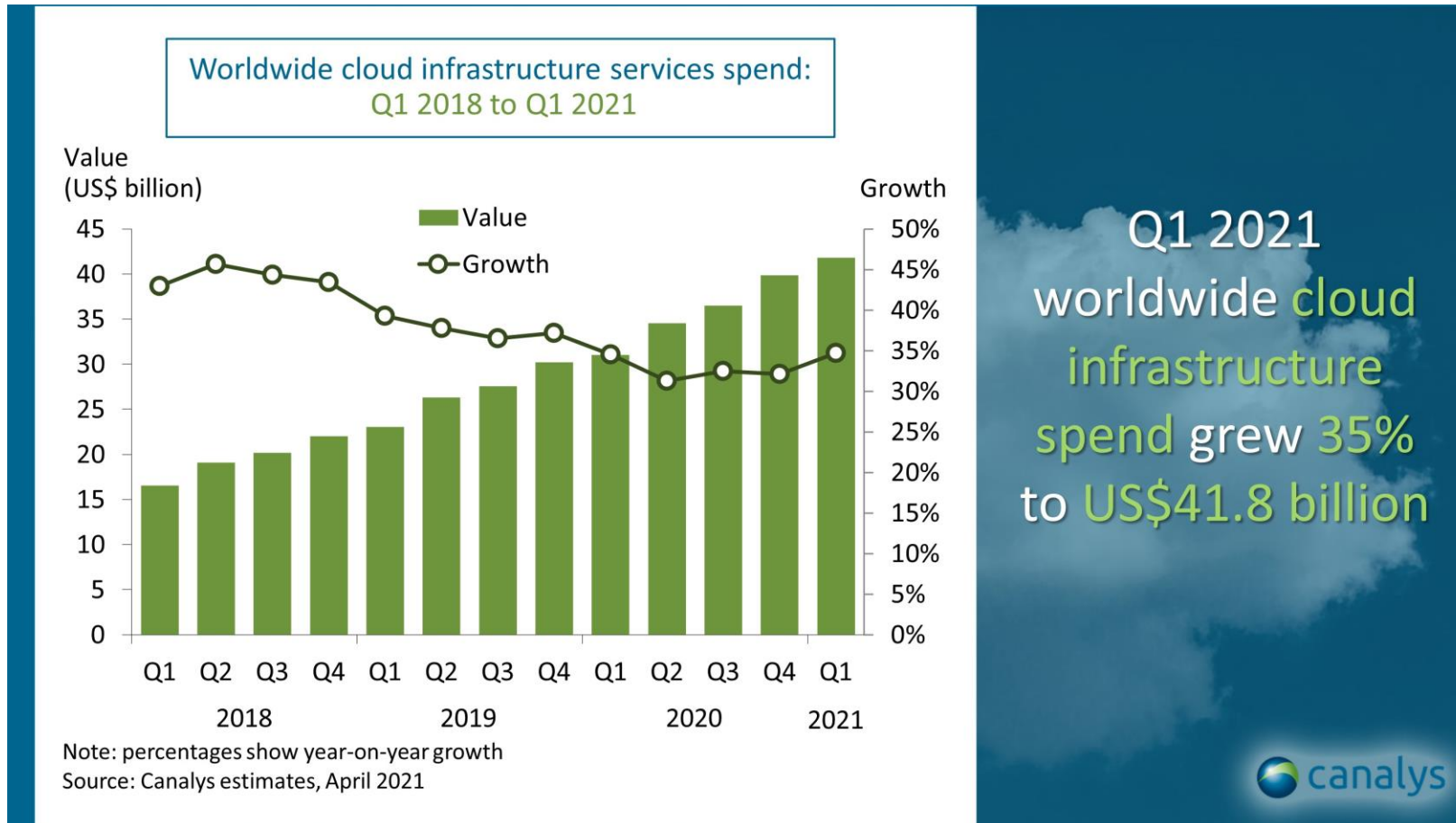
Felhő biztonsági kérdések aktualitásai

Dr. Kovács Zoltán
Vodafone Magyarország zrt.

c1

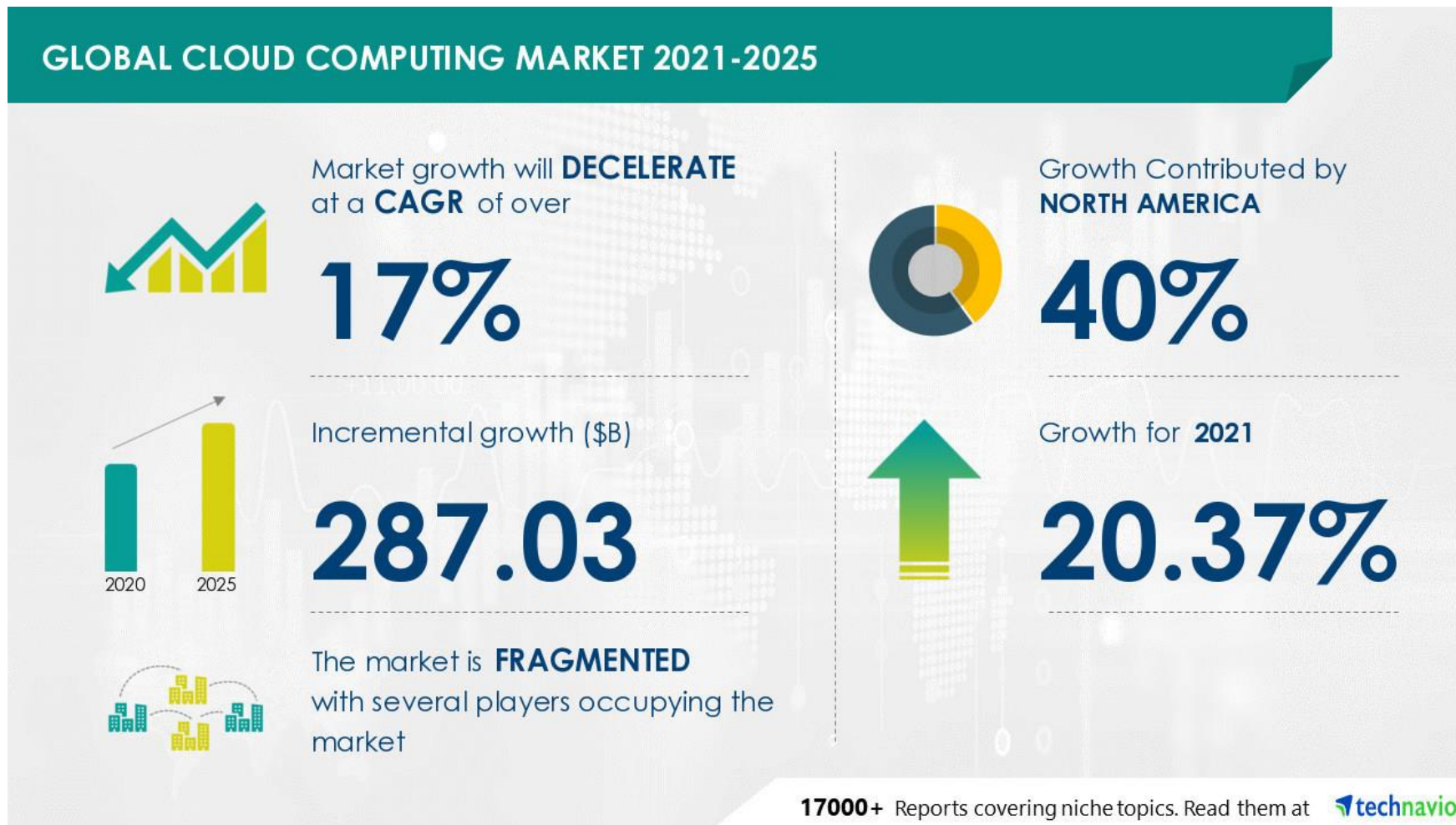


Felhő megkerülhetetlensége

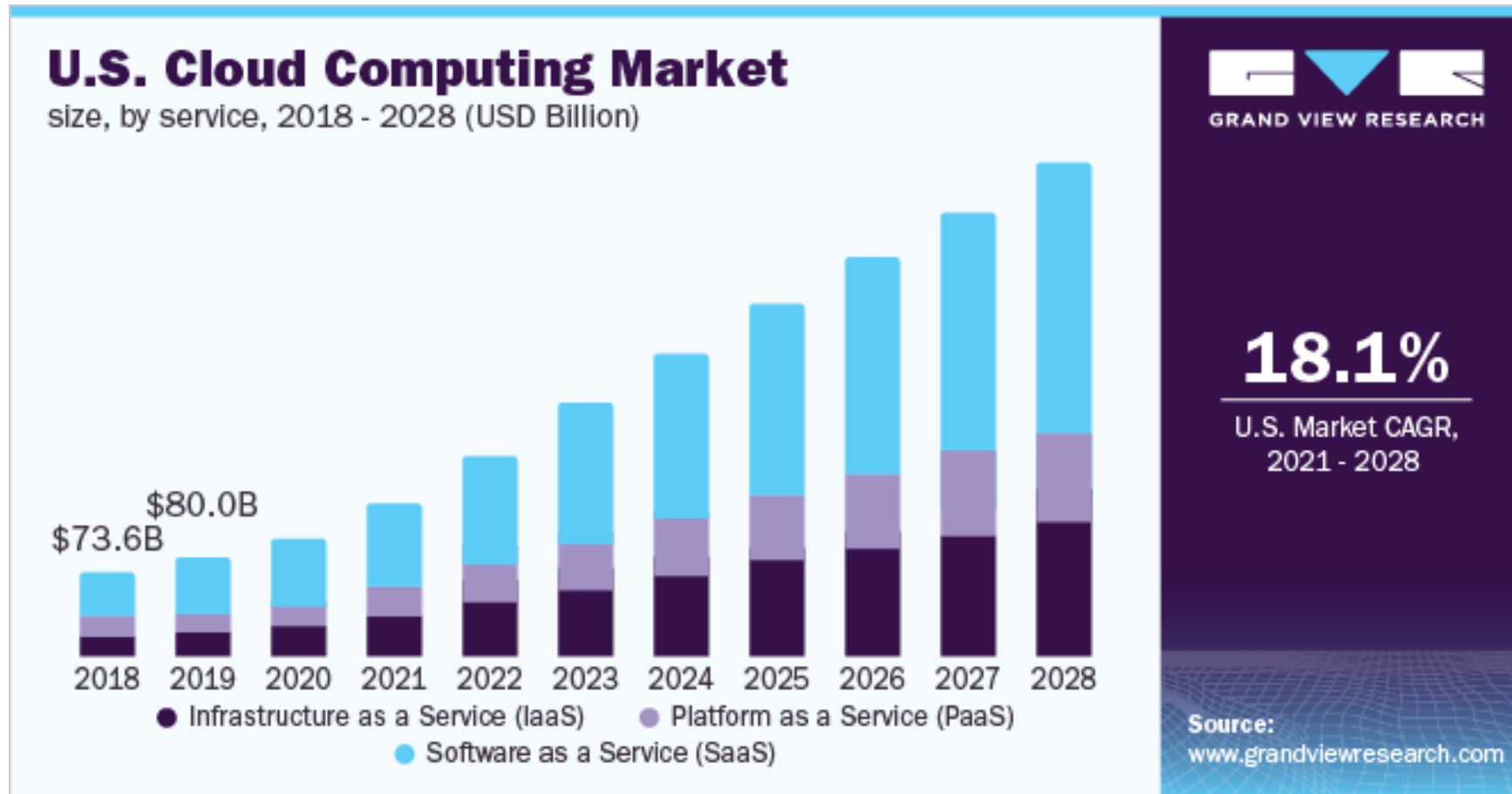


Forrás: <https://canalys.com/newsroom/global-cloud-market-Q121>.

Felhő megkerülhetetlensége



Felhő megkerülhetetlensége



Forrás: <https://www.grandviewresearch.com/industry-analysis/cloud-computing-industry>.

Felhő biztonsági problémák

Új biztonsági kihívások, pl.:

- **adatokkal kapcsolatos biztonsági megfontolások** (tulajdonjog, adatok migrációja, adatok biztonsága és adatvédelem, biztonsági tesztek célja és hatálya, hibajavítások, adatmegőrzés és törlés, interoperabilitás, stb.),
- **a kínált és szükséges biztonsági intézkedések** (hozzáférési pontok, biztonsági értékelések és jogosultságok, folyamatos ellenőrzés, biztonsági ellenőrzések implementálása stb.),
- a felhőben használt **virtuális operációs rendszerek biztonsága**,
- **titkosítás** szükségessége a felhő használatához, a felhő erőforrások felügyeletét szabályozó interfész, operációs rendszerek, alkalmazások, adatok eléréséhez,
- **adatok tulajdonjoga**,
- több-felhasználós környezet problémái, **izoláció**,
- **naplózási** kérdések,
- **adatmegőrzési** kérdések (az adataink valóban törlésre kerüljenek, azok ne legyen visszaállíthatóak, még a back-up-ból sem)
- **szolgáltató kémkedésének** kérdésköre,
- **3 fél bevonása** (a szolgáltató olyan alvállalkozói, akikkel a felhasználónak nincs szerződése)

Vizsgálandó kérdések

Üzembiztonság

- közösségi felhő közös üzembiztonsági alapkövetelményei
- hordozhatóság és interoperabilitás
- üzletmenet-folytonosság
- rendelkezésre állás, ellenálló-képesség, megbízhatóság
- szolgáltatási szintek, azok garanciái
- skálázhatóság és erőforrás menedzsment
- redundancia
- katasztrófa-elhárítási terv
- biztonsági mentés és visszaállítás
- életciklus kezelés és változásmenedzsment
- adatmigráció
- adatformátum
- adatközpont működés, rendszer konfiguráció
- alkalmazásbiztonság
- javítócsomagok kezelése
- ellátási lánc üzembiztonsága
- üzembiztonsági kockázatcsökkentési terv

Adatbiztonság

- közösségi felhő közös üzembiztonsági alapkövetelményei
- irányítás
- kockázatkezelés
- azonosítás, hitelesítés jogosultságkezelés és hozzáférés szabályozás
- határvédelmi eszközök működtetése és ellenőrzése
- folyamatos ellenőrzés
- incidenskezelés
- sérülékenységi vizsgálat, kezelés
- titkosítás és kulcskezelés
- virtualizációból adódó biztonság kezelése
- kliensoldali védelem
- vezeték nélküli hálózatok biztonsága
- biztonsági architektúra
- adatok elvesztése, ellopása
- mobil eszközök kezelése

Egyéb (jogi, fizikai stb.) biztonság

- jogi megfelelés
- fizikai biztonság
- személyi biztonság
- gazdasági biztonság
- dokumentumbiztonság

Biztonsági elemző sablon

Kategóriák vizsgálandó kérdései	válaszok	
	igen	nem
Üzembiztonság:		
1. közösségi felhő közös üzembiztonsági alapkövetelményei		
A felhasználó számára megfelelő és elfogadható a közösségi felhő felhasználói által kialakított közös üzembiztonsági alapkövetelmény rendszer?	☐	☐
2. hordozhatóság és interoperabilitás		
A szolgáltató által kínált eszközök, rendszerek és szolgáltatások biztosítják az adatok hordozhatóságát és a különböző (szolgáltató, felhasználó, harmadik fél) rendszereinek együttműködését?	☐	☐
A szolgáltató által kínált eszközök, rendszerek és szolgáltatások biztosítják az együttműködési képességet más, saját országbeli érintett hatóság vagy közigazgatási szervvel?	☐	☐
A szolgáltató által kínált eszközök, rendszerek és szolgáltatások biztosítják az együttműködési képességet más országok vagy EU érintett rendvédelmi szerveinek rendszereivel?	☐	☐
◦ A szolgáltató nyilvános, publikált API-kat használ?	☐	☐
◦ A szolgáltató által kínált interfészek interoperabilisak		
▪ a felhasználó rendszereinek interfészeivel?	☐	☐
▪ a felhasználó munkafolyamataihoz kapcsolódó harmadik felek rendszereinek interfészeivel?	☐	☐

Felhő a privát és az állami szférában

Kormányzati felhő:

- Saját kormányzati felhő megoldás
 - Nagyon sok biztonsági problémát kezel
 - Előremutató, példa értékű koncepció
- Jelentkező kihívások:
 - Nehéz mindent ide bevinni
 - Meghatározott kör használhatja – hiszen ez a deklarált célja!
 - Továbbfejlesztések korlátozottabbak, mint nem állami esetében
 - Sokszor használnak a jogosultak is nem kormányzati felhőt, - akár úgy használják a munkatársak, hogy nem is tud róla vezetés
- Összegezve: biztonsági szempontból más problémák, de lényegesen egyszerűbb kérdés

Kibertámadás a FUJITSU PROJECTWEB ellen

- A Fujitsu ProjectWEB egy felhő alapú szoftver, vállalatok online együttműködéséhez, szoftvermenedzsmenthez és fájlmegosztáshoz.
- Az eszköz népszerű a japán kormányzati szervek körében.
- 2021. májusában a támadók hozzáfértek japán kormányzati adatokhoz.
- A japán légiforgalom irányítás adatait is ellopták a támadásban.



Kibertámadás az ellátási lánc ellen



- Az ellátási láncot ért **támadások 2021-ben** várhatóan **4-szeresére nőnek 2020-hoz képest.**
- Az incidensek kb. **58%-ánál** a támadás célja az **ügyféladatokat** (beleértve a személyazonosításra alkalmas adatokat) és a **szellemi tulajdont** tartalmazó eszközök **ellen irányult!**
- A támadások **66%-ánál a beszállítók nem tudták, vagy nem jelentették** az incidenst.
- **Más** a kiberbiztonsági, ezen belül az incidensek jelentésének **érettsége** az ellátási lánc szereplői között!

Ellátási lánc, felhő, kibertámadás....

- Vállalatok önállóan szerződnek
- Vagy többszörös kiszervezés – egy már kiszervezett tevékenység – a szolgáltató cég tovább szerződik
- Ellátási lánc támadása - kérdések
 - Ki a felelős?
 - Hogyan lehet védekezni ez ellen?

5G Campus Network

Kitekintés

Individual networks for companies

Medium-sized enterprises

5G priváthálózatok

más biztonsági kihívások – fokozott biztonság kell minden szereplőtől!

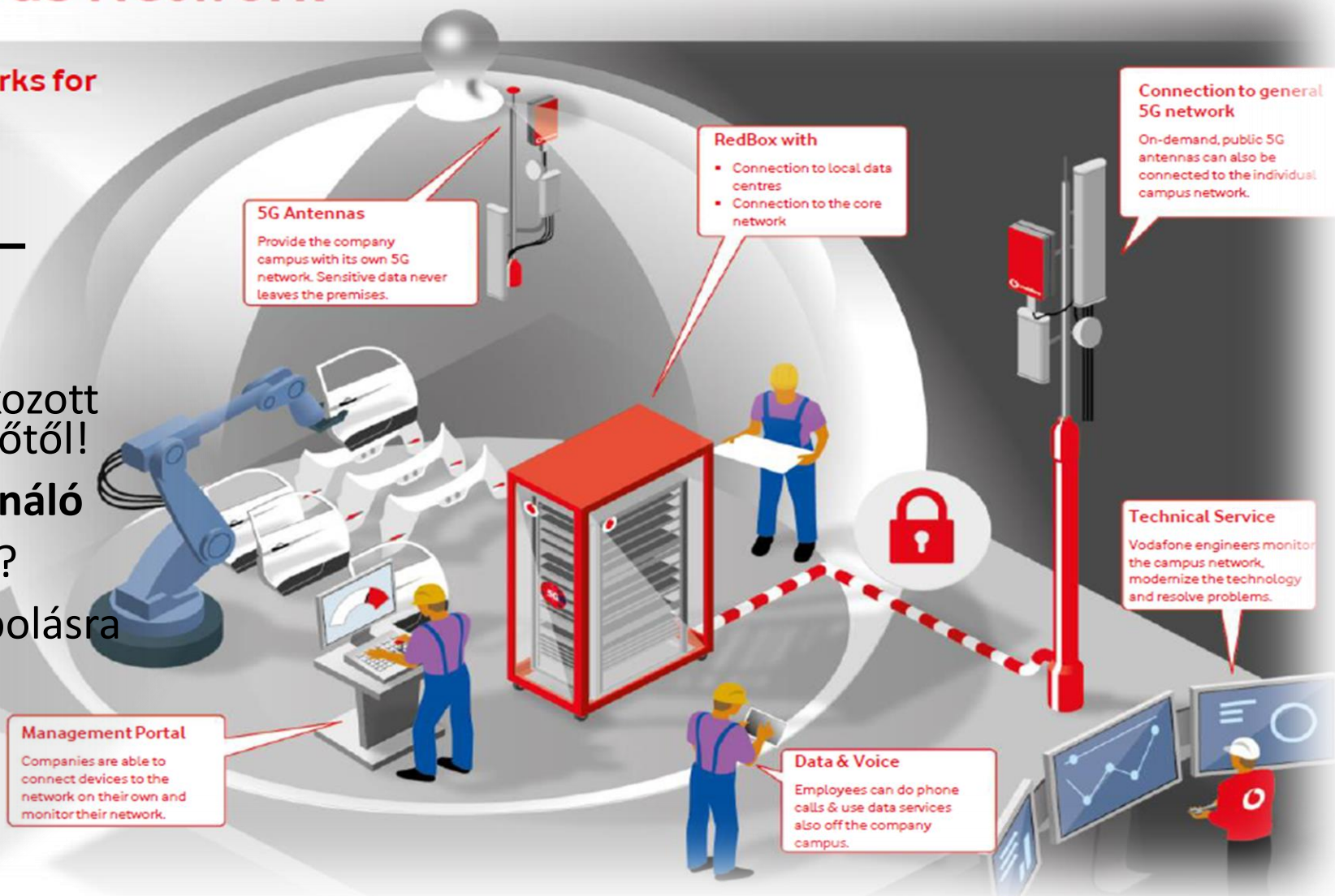
Szolgáltató ☒

Felhasználó

5G Security toolbox

???

itt egy támadás akár hard rombolásra is alkalmasak lehet!!!



AI használata a kibertámadásoknál és a kibervédelemben

Támadó és védő oldalon is megjelenik már

RSA Conf 2019 – demo támadó AI vs. védő AI

FireEye CYBER DEFENSE
SUMMIT 2018 – kb. 5 éven belül az L1 operátorok munkáját felváltja AI

Tapasztalat – használják mindkét oldalon már

AI és felhő használata a fraud elleni küzdelemben

Multi vállalatnál

- Előnyök:
 - AI és gépi tanulás hatékony használata
 - Nemzetközi információs bázis a betanuláshoz
 - Mindenhol a legjobb szabályok beépíthetők
 - Ha valahol megjelenik új csalási forma
 - Felismerés
 - Szabály a kivédésére
 - Más opcióknál azonnal megjelenik

További lehetőségek

Működhet akár iparágra is – fő kérdés: bizalom – beadom az adataimat?

- Ágazati TIP?
- Ágazati anti-fraud platform?



Together we can