INFORMÁCIÓS RENDSZEREK ÜZEMELTETÉSE

BME VIK TMIT

MÉRNÖK-INFORMATIKUS ALAPKÉPZÉS

7. VIRTUALIZÁCIÓ, FELHŐ

Virtualizáció és felhő IT. A felhő IT alapelvei. A migráció kérdései. Együttműködtethetőség. Szabványosítási irányok. Előnyök és kockázatok, Monitoring. Hozzáférés-szabályozás.

A RENDSZERÜZEMELTETÉS TIPIKUS FELADATAI

- IT rendszer tervezése, telepítése, konfigurálása
- Tároló, hálózati és más rendszer-komponensek tervezése, méretezése, létrehozása
- Rendelkezésre állásra tervezés (High Availability and Disaster Recovery)
- IT rendszer monitorozása, fenntartása
- Rendszerhangolás (a monitorozás alapján)
- Terhelés-szabályozás (re-balancing workloads)
- Biztonságos működés megoldása (rendszer, hálózat, eszközök), a követelmények és az implementáció alapján
- IT biztonsági tervezés, ellenőrzés (user and account security rights and restrictions)

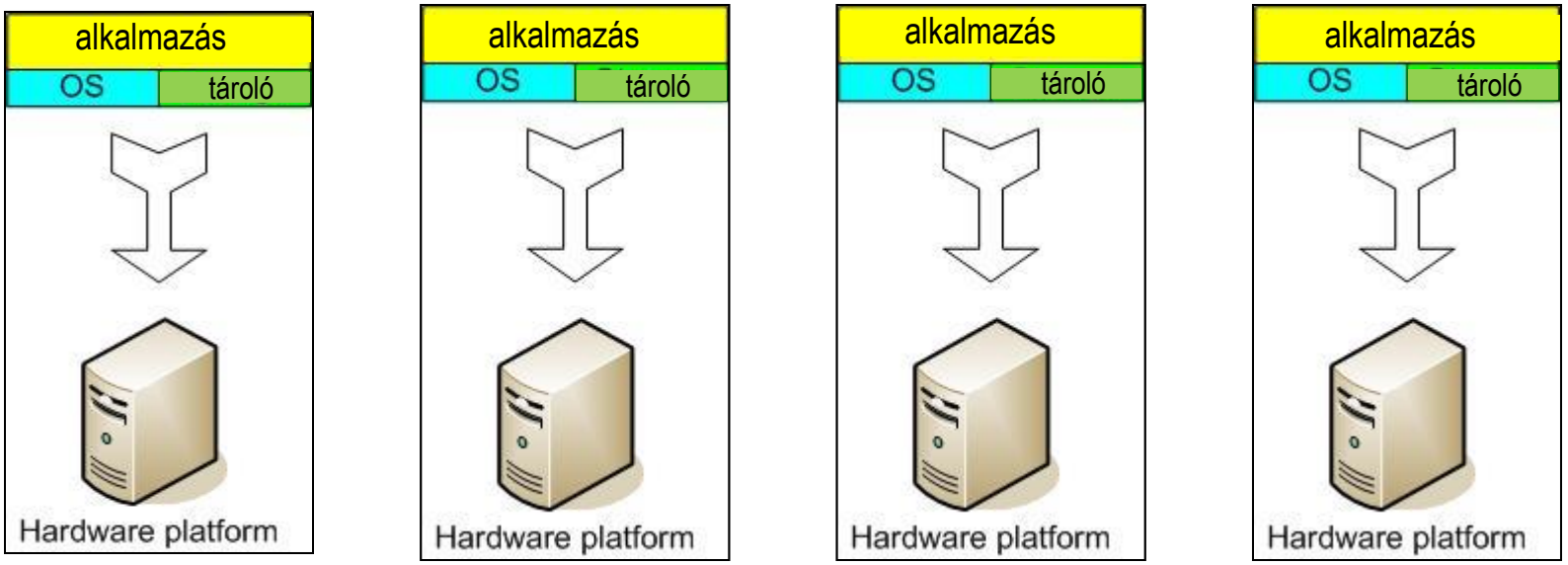
Mi változik a rendszerüzemeltetés feladataiból a felhő architektúrában?

- Kevesebb feladat a helyi (on-site, on-premise) IT rendszertervezés, telepítés, konfigurálás, monitorozás, ellenőrzés területein.
- Erőforrás-gazdálkodás virtualizált környezetben (virtuális gépek, IaaS)
- Ha van kód/alkalmazás-fejlesztés: felhő platform biztosítása (menedzselése)
- Változó IT biztonsági megoldások
- Változó migrációs feladatok
- stb.

VIRTUALIZÁCIÓ ÉS FELHŐ IT (CLOUD COMPUTING)

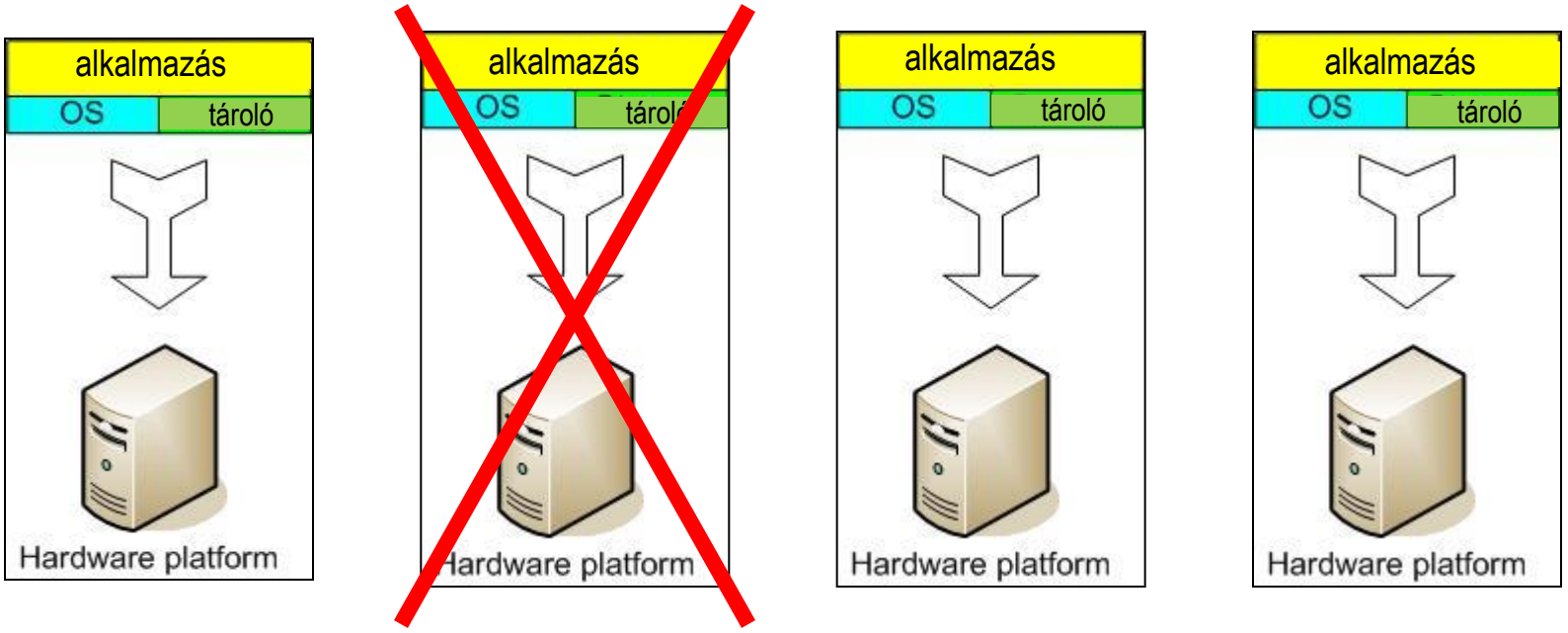
- Virtualizáció:
  az a képesség, hogy egy fizikai rendszeren több(féle) operációs rendszer futtatható
  (és megosztják a rendelkezésre álló erőforrásokat)
- Felhő IT:
  Szolgáltatások kívánság szerint, az erőforrások le/felskálázásával

NÉZZÜNK EGY PÉLDÁT: HAGYOMÁNYOS SZERVER KONCEPCIÓ



webszerver	alkalmazás-szerver	DB szerver	e-mail
Windows	Linux	Linux	Windows
IIS		MySQL	Exchange

… HA VALAMELYIK ELROMLIK:



webszerver

Windows

IIS

az alkalmazás szerver leáll

DB szerver

Linux

MySQL

e-mail

Windows

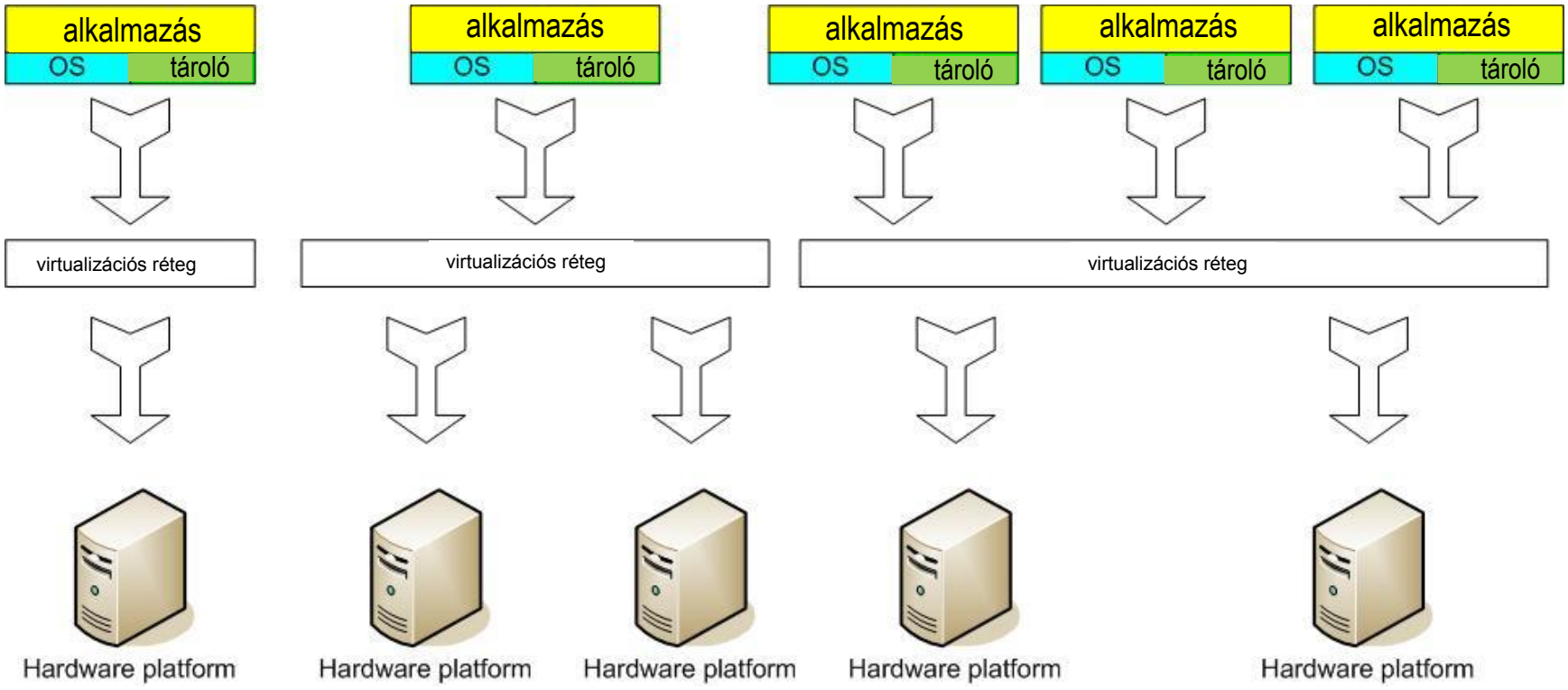
Exchange

A HAGYOMÁNYOS SZERVER KONCEPCIÓ

a szerver itt olyan egység, amiben benne van a hardver, az op. rendszer, a tároló és az alkalmazások; a szerverekre gyakran szolgáltatásaik szerint hivatkoznak (levelező, adatbázis, fájl szerver, stb.); az egység hibája esetén a szolgáltatás leáll;
hibatűrő megoldásokkal a leállás esélye csökkenhető

- előnyei
  - könnyű tervezni
  - könnyű megvalósítani
  - könnyű menteni (backup)
  - virtuálisan bármely alkalmazás/szolgáltatás futtatható ilyen telepítésben
- hátrányai
  - viszonylag drága felállítani és karbantartani a hardvert
  - nem nagyon skálázható
  - nehéz másolni (replicate) a konfigurációt
  - redundanciát viszonylag nehét implementálni
  - hardver üzemszünet miatt sebezhető
  - a processzor kihasználtsága gyakran alacsony

VIRTUÁLIS SZERVER KONCEPCIÓ



Virtuális gép réteg a felhasználói („vendég”) op. rendszer és a hardver között

A VIRTUÁLIS SZERVER KONCEPCIÓ

logikailag elválasztja a szerver szoftvert a hardvertől

  – a szerver szoftverbe beleérthetjük az op. rendszert, az alkalmazásokat és a tárolást is

- Egy virtuális szervert egy vagy több host is megvalósíthat és fordítva: egy host több virtuális szervert is magába foglalhat.
- A virtuális kiszolgálókat (is) funkció szerint szokás hivatkozni (levelező, adatbázis, fájl szerver, stb.).

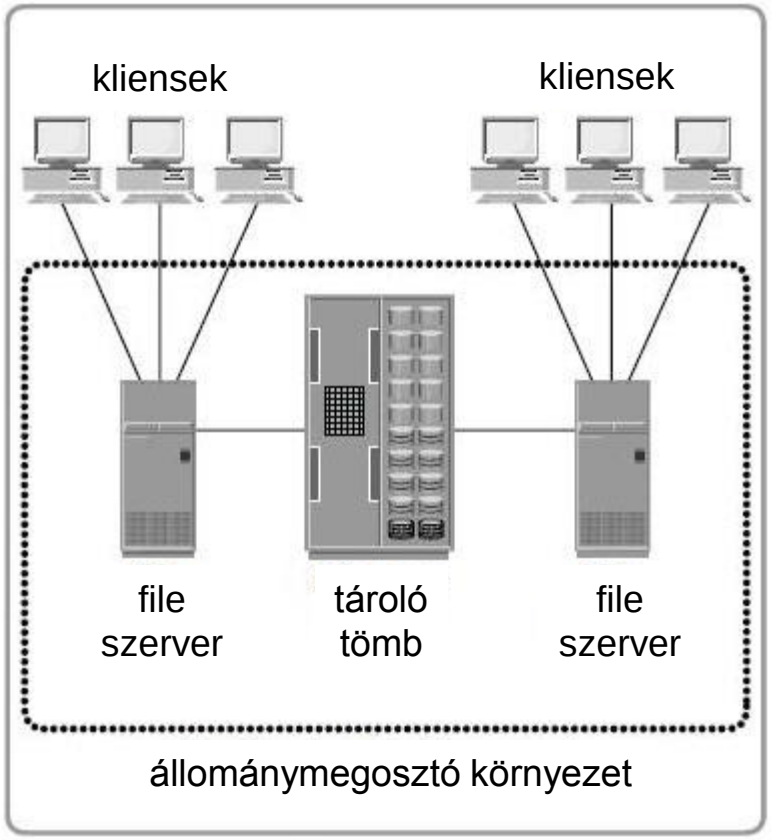
A VIRTUÁLIS SZERVER KONCEPCIÓ

szolgáltatásai (jó tervezéssel) nem szünetelhetnek egy host kiesésével (ezzel pl. a karbantartás és a hardver upgrade is leállítás nélkül elvégezhető)
könnyen skálázható (szükség szerint allokálható erőforrás)
szerver mintákkal (templates) többszörözhető
hostról hostra könnyen telepíthető

- előnyei
  - közös erőforrás gazdálkodás (Resource pooling)
  - redundancia
  - magas rendelkezésre állás
  - új szerver gyors telepítése
  - leállás nélkül átkonfigurálható
  - fizikai erőforrások optimalizálása gazdaságos
- hátrányai
  - bonyolultabb tervezés
  - drágább konfiguráció, mint a hagyományos (ugyanúgy meg kell a hardvert, az OS-t, az alkalmazásokat + az absztrakciós réteget is)

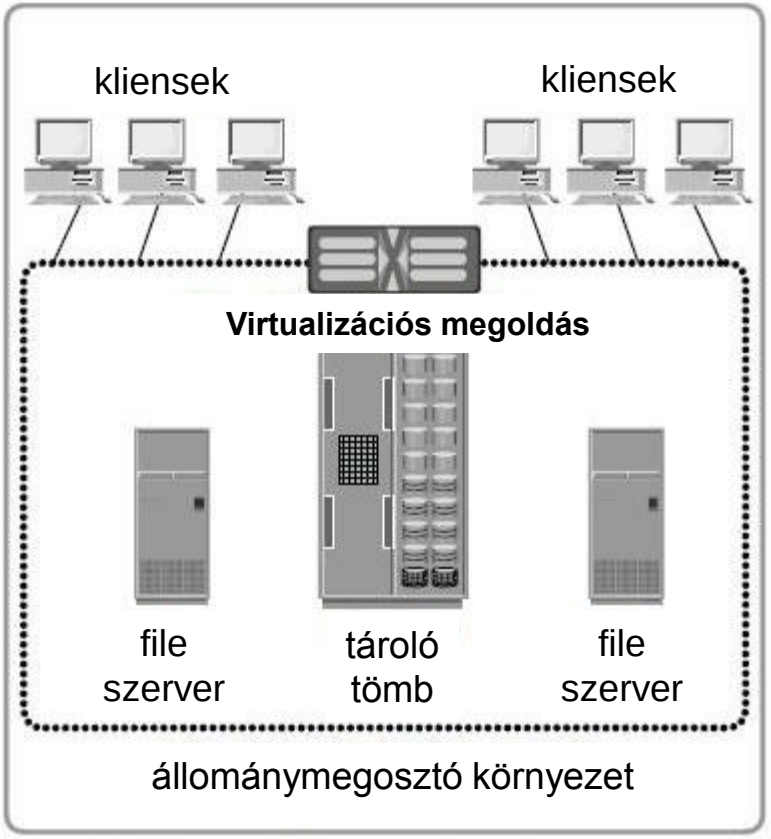
FÁJLSZINTŰ VIRTUALIZÁCIÓ

- Fájlszintű virtualizáció nélkül
  - egy kliens/host egy fájlt szeretne elérni egy adott fájlszerveren
  - tudnia kell, hogy melyiken
  - lehet, hogy az egyik szerver tele, a másik üres
  - fájl mozgatás érinti a klienst is

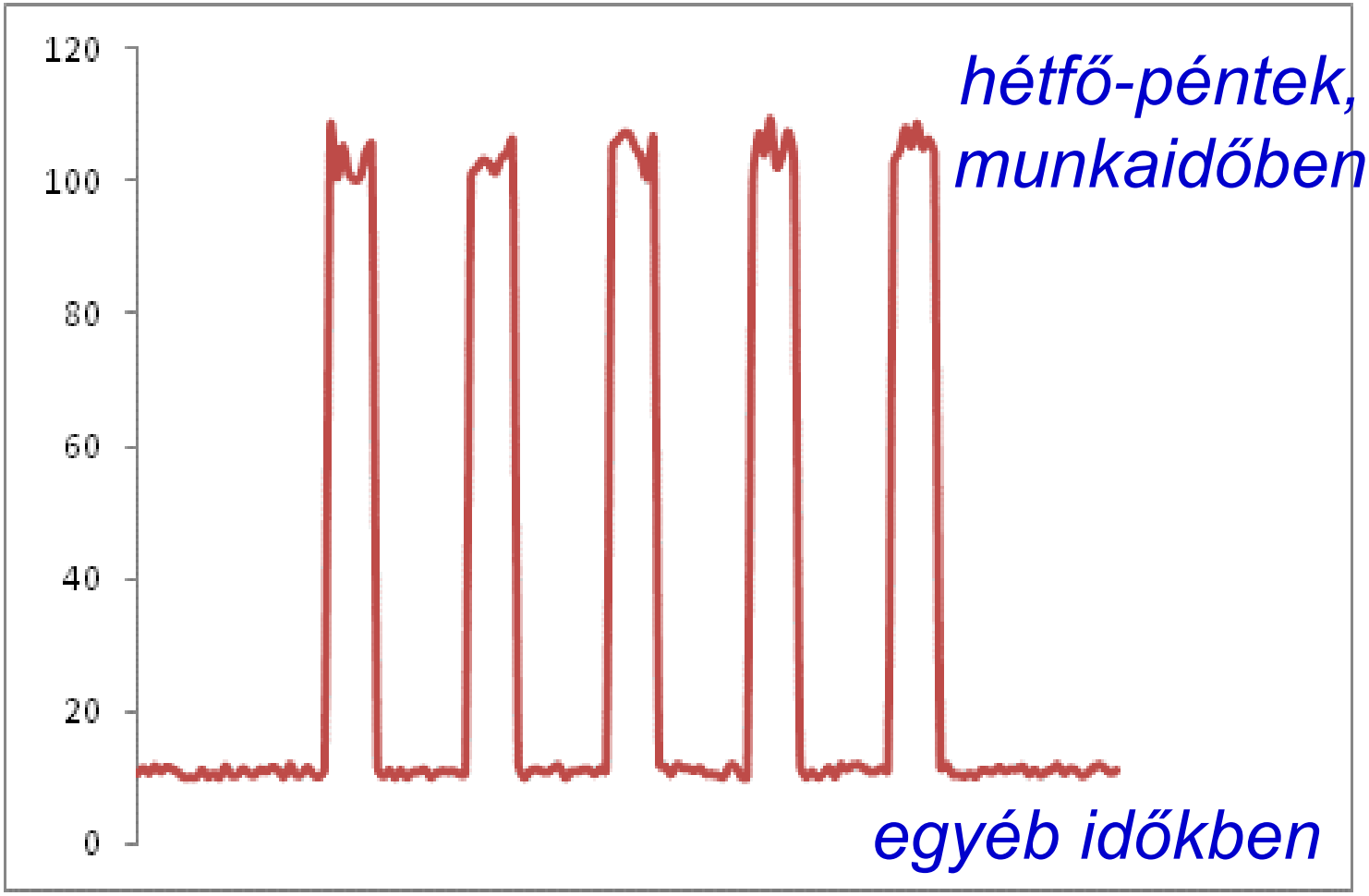


FÁJLSZINTŰ VIRTUALIZÁCIÓ

- Virtualizált fájlszerver
  - a kliensnek nem kell tudni, melyik fizikai szerveren van a fájl
  - egyszerűbb
    - terhelésmegosztás
    - fájlmozgatás
    - bővítés
- Cloud Computing



HAGYOMÁNYOS SZOLGÁLTATÓI IT RENDSZER FORGALMI DIAGRAMJA



A VIRTUALIZÁCIÓ KÖVETKEZŐ LÉPÉSE A FELHŐ IT

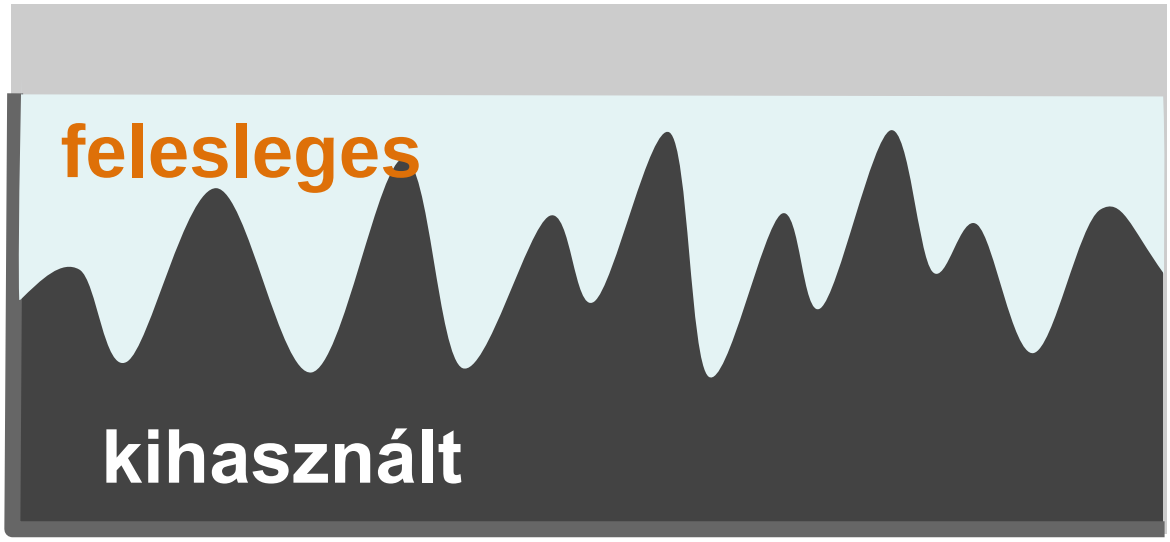
- Nem kell saját hardverrel rendelkezned.
- Bérelheted a „felhőből”.
- Nyilvános, privát, vagy hibrid felhő IT.

A FELHŐ IT (CLOUD COMPUTING)

felhasználás alapján fizetett IT erőforrás igénybe vételi modell.

Hálózati hozzáférés egy megosztott IT erőforrás készlethez (pl., szerverek, tárolók, alkalmazások, szolgáltatások), amit (a szükséges verzióban) gyorsan lehet biztosítani, kevés szolgáltatói interakcióval.

SAJÁT IT ERŐFORRÁSOKKAL:

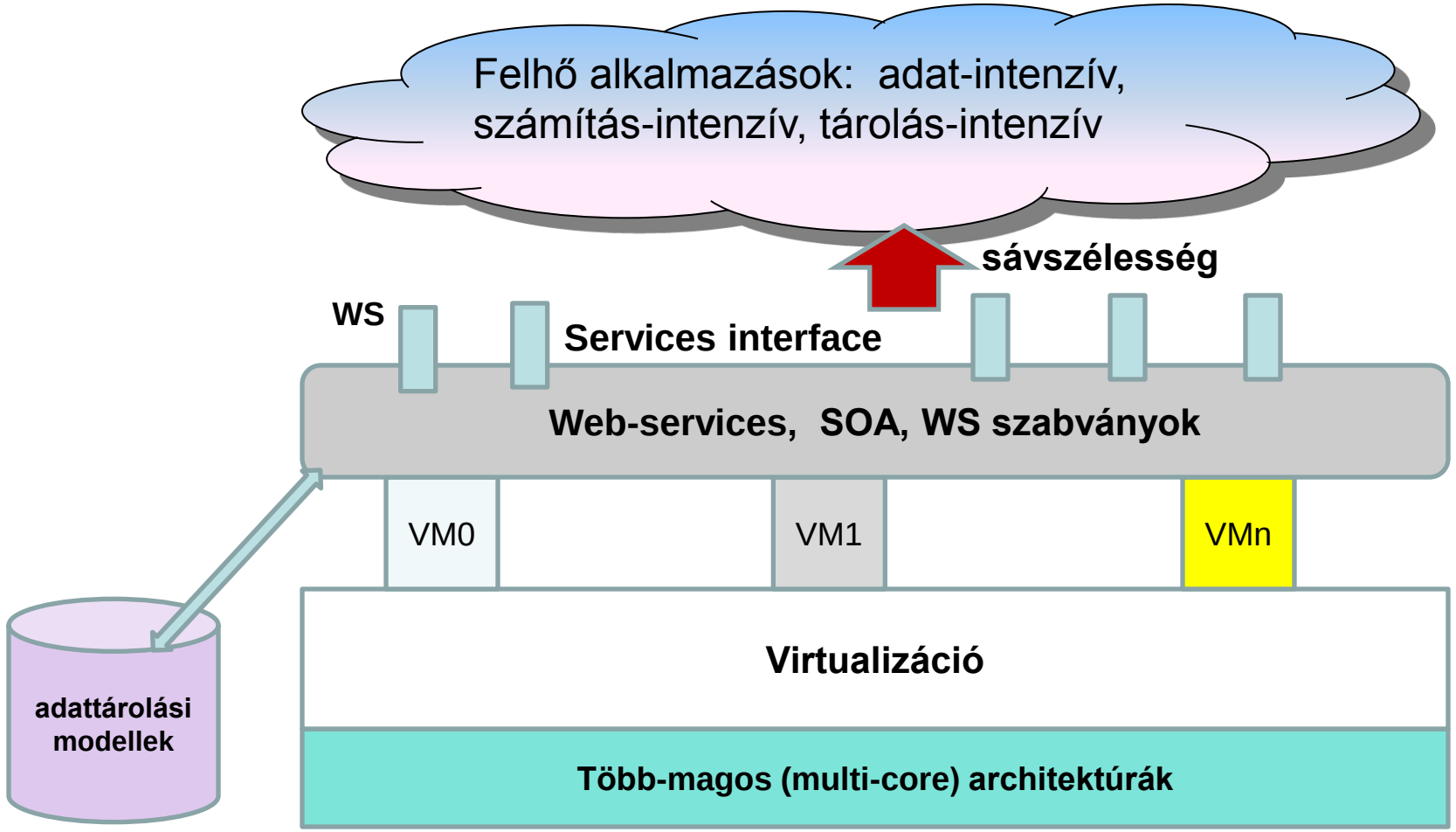


Felhő IT megoldásban:

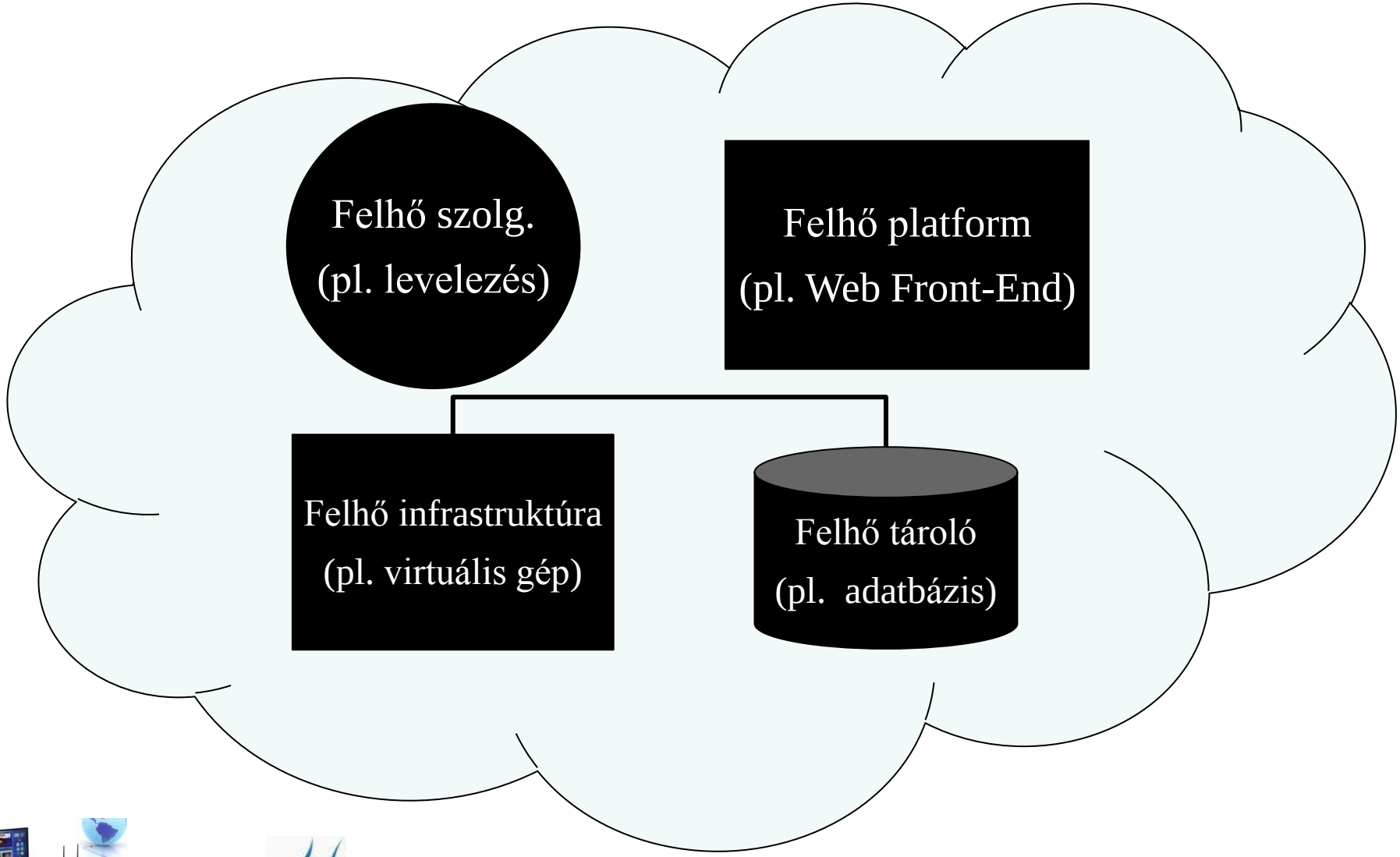
LEGFONTOSABB FELTÉTELEI

	Mit értünk alatta?
Univerzális hozzáférés	A felhő IT szolgáltatásai legyenek mindenütt igénybe vehetők (ubiquitous) – munkaállomásról, mobil eszközről, telefonról, céleszközről
Skálázható szolgáltatások	Fel/leskálázás, az ezt vezérlő infrastruktúrával. Üzletvezérelt erőforrás-allokálás: a tőke és a működési költségek alapján fogják megítélni, hogy mi/mennyi szükséges.
Új alkalmazás-szolgáltatási modellek	Párhuzamos és folytonos szolgáltatások is lehetnek.

„ENGEDÉLYEZŐ” TECHNOLÓGIÁK



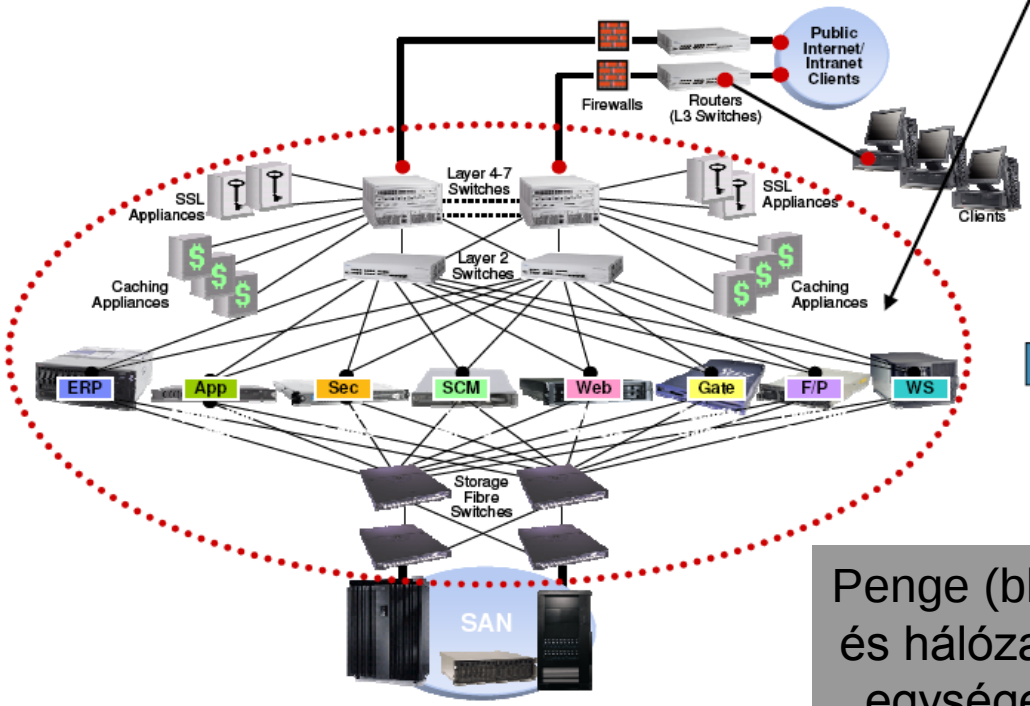
EGYSZERŰ FELHŐ IT MODELL



AMI AZ EGYSZERŰ MODELL MÖGÖTT VAN: **ADATKÖZPONT TOPOLÓGIA**

Cél: a funkció-specifikus elemek helyett virtuális egységek közös keretben és hálózatban

HAGYOMÁNYOS TOPOLÓGIA



FELHŐ TOPOLÓGIA

Penge (blade) számítási és hálózati eszközök, egységes keretben

ALAPELVEK

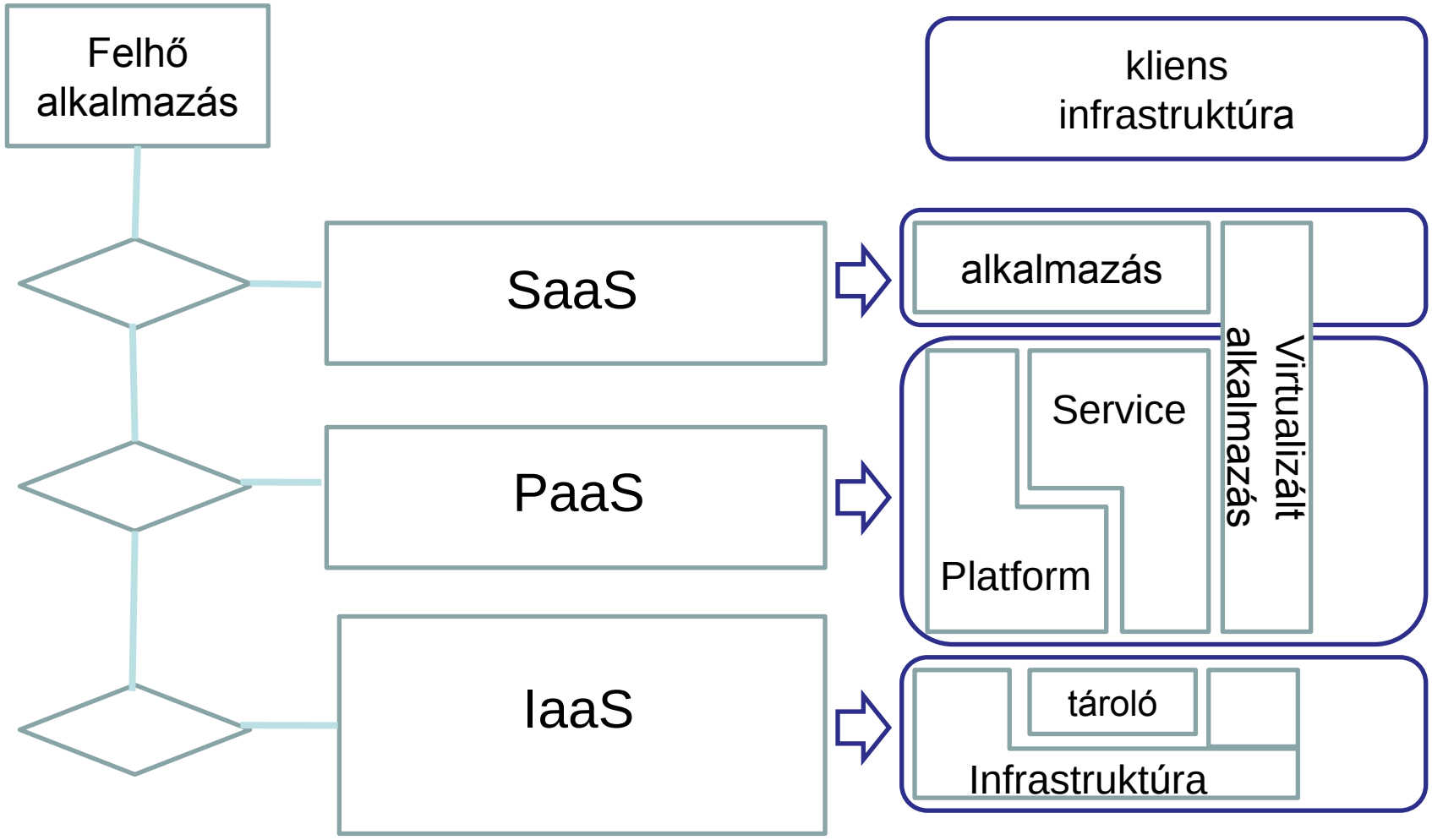
- Internet protokollokkal elérhető bármely számítógépről.
- Mindig elérhető és az igényekhez igazítható.
- Felhasználás szerint fizetett (pay per use). (változatos árazás a gyakorlatban)
- Vezérlő/ellenőrző interfészek.
- „Önkiszolgáló”

National Institute of Standards and Technology (NIST) definíció:

"pay-per-use” (fizesd-amit-használsz) modell létező, kényelmes és igény-szerinti hálózati hozzáférés engedélyezésére konfigurálható IT erőforrások (hálózatok, szerverek, tárolók, alkalmazások és szolgáltatások) megosztott készletéhez, amelyek könnyen létesíthetők és változtathatók minimális menedzsment erőfeszítéssel vagy szolgáltatói interakcióval.”

… *AKÁRMI*-AS-A SERVICE

- Data-as-a-service
- Storage-as-a-service
- Database-as-a-service
- Information-as-a-service
- Process-as-a-service
- Application-as-a-service
- Platform-as-a-service
- Integration-as-a-service
- Security-as-a-service
- Testing-as-a-service
- Infrastructure-as-a-service

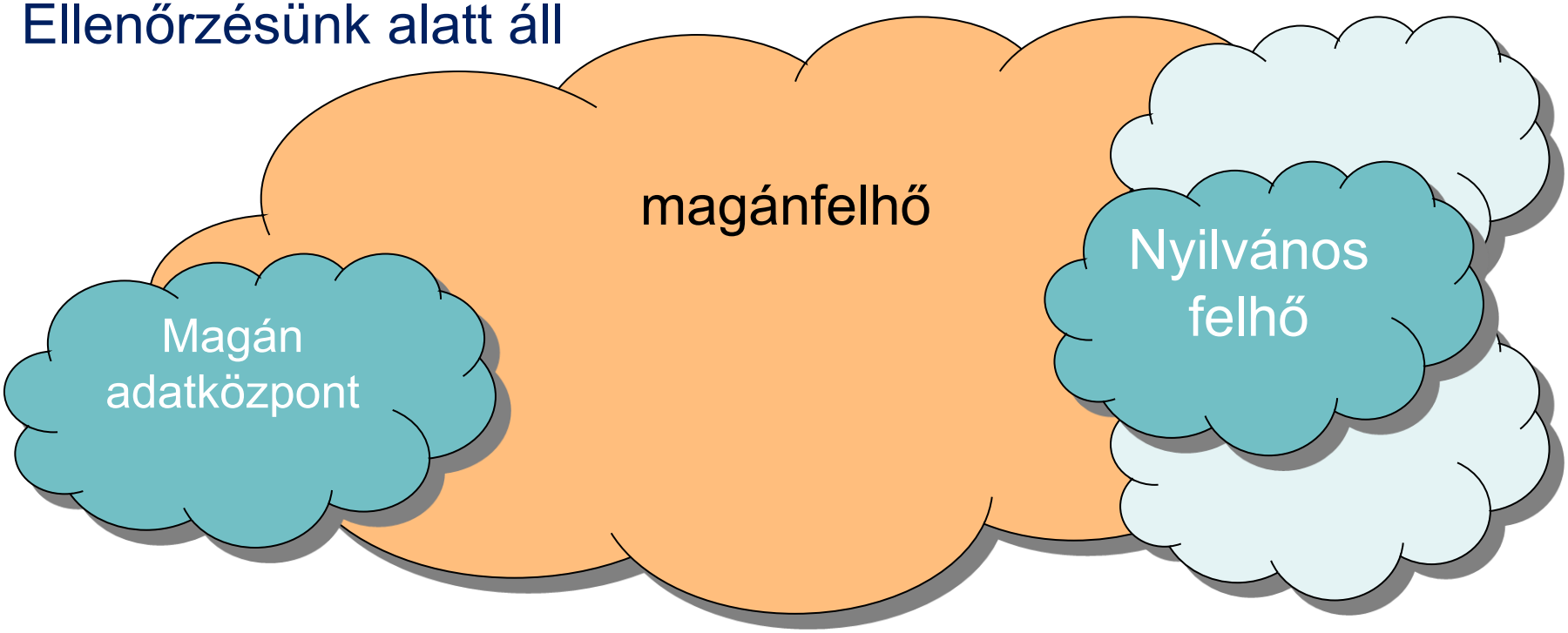

Felhő alkalmazás
kliens infrastruktúra
SaaS
PaaS
IaaS
alkalmazás
Virtualizált alkalmazás
Service
Platform
tároló
Infrastruktúra

TÍPUSAI

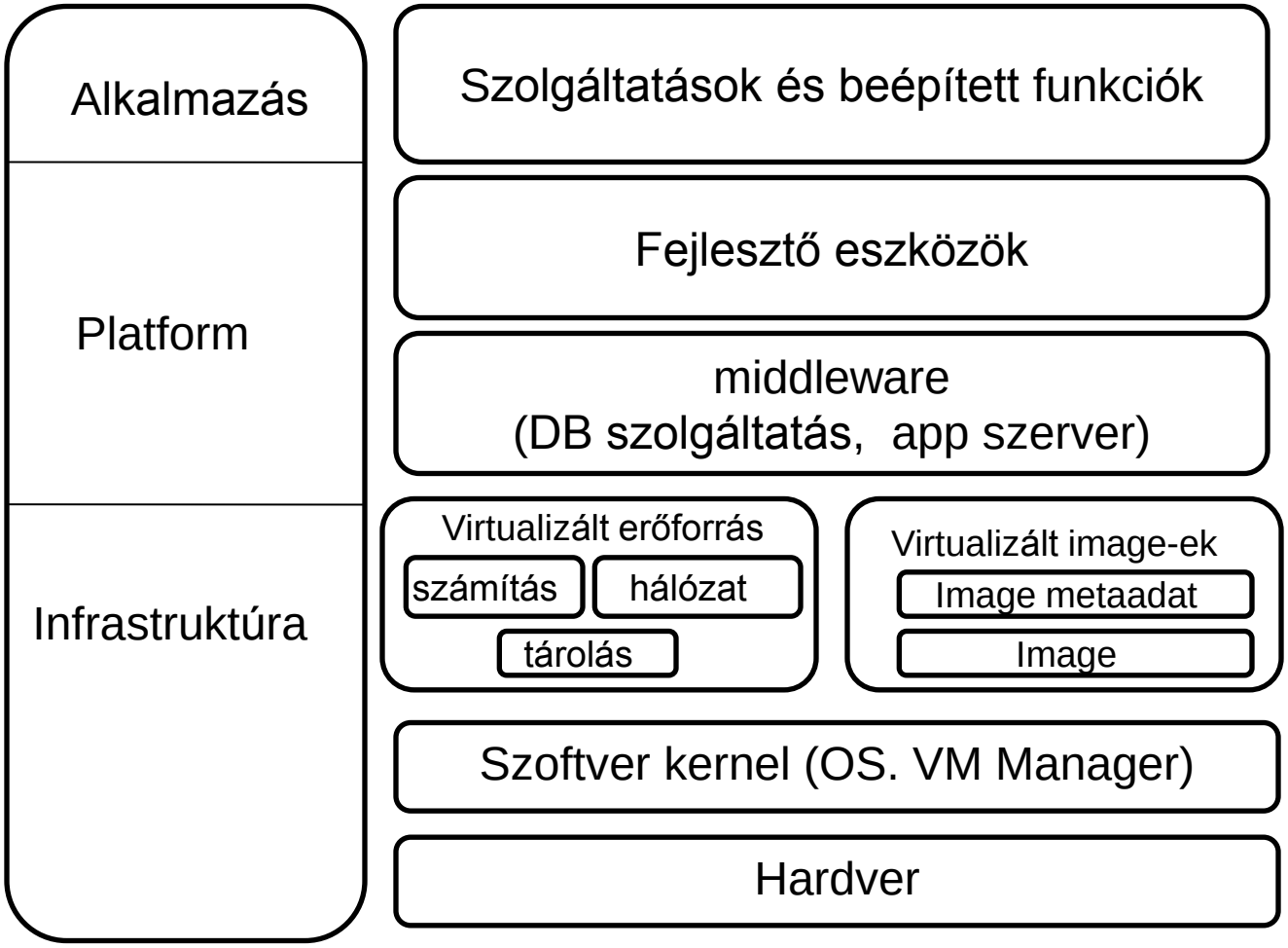
- Nyilvános felhő (Public Cloud)
- Magánfelhő (Private Cloud)
- Hibrid felhő (Hybrid Cloud)

Biztonságos
Megbízható
(bízunk benne)
Ellenőrzésünk alatt áll

Rugalmas
Dinamikus
Igénybevétel szerint
Hatékony

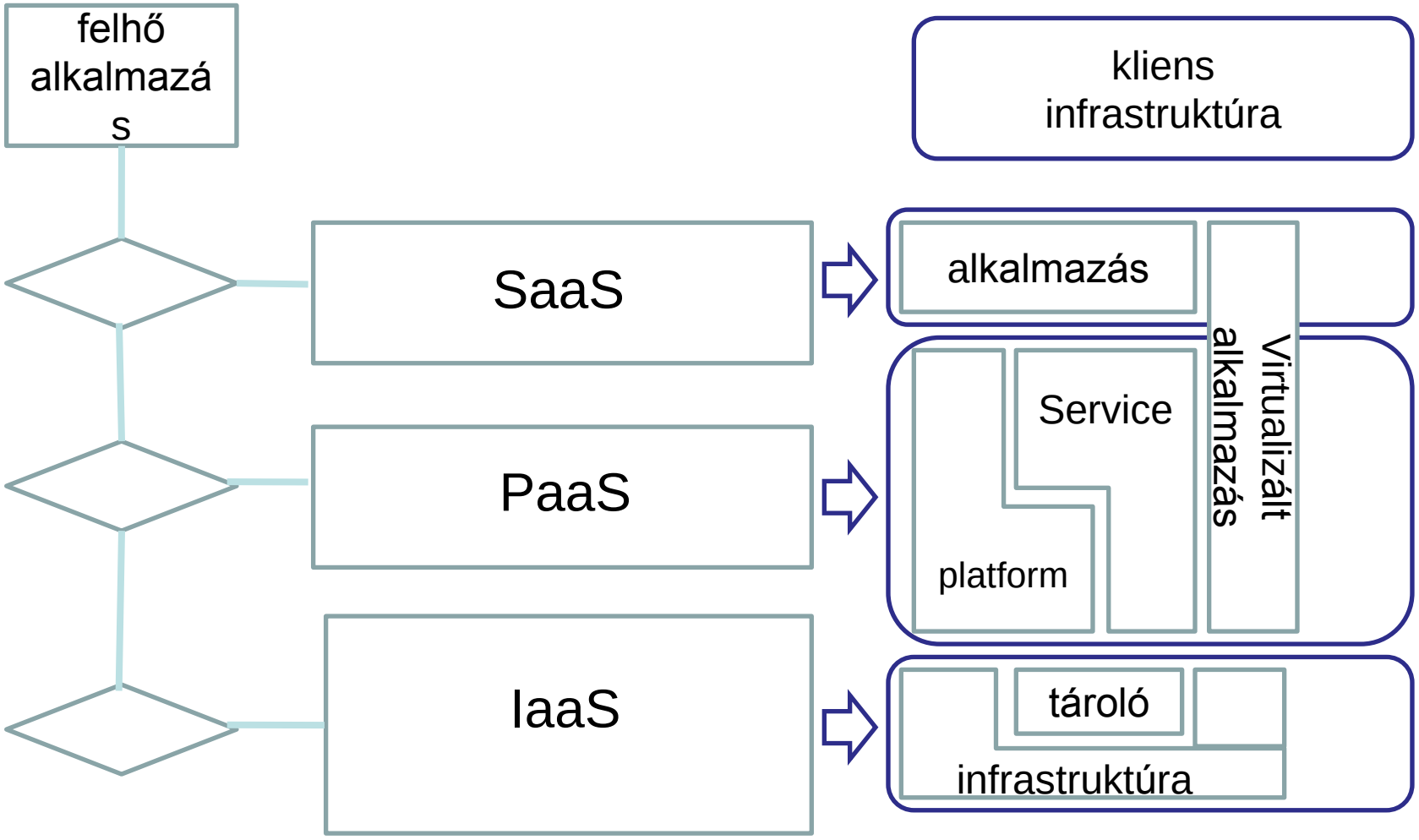


MIT ADUNK EL A KÜLÖNBÖZŐ SZOLGÁLTATÁSI SZINTEKEN?



VIRTUALIZÁLT INFRASTRUKTÚRA MENEDZSMENT A FELHŐBEN

- Sokféle követelmény menedzseléséhez a virtualizált erőforrások egységes és homogén nézete kell
- Virtuális infrastruktúra menedzsment (Virtual Infrastructure Management)
  - VM-ek menedzselése különböző fizikai host-okon
  - Távoli biztonságos interfész vezérléshez és monitoring-hoz (IaaS)


felhő alkalmazás
kliens infrastruktúra
SaaS
PaaS
IaaS
alkalmazás
Virtualizált alkalmazás
Service
platform
tároló
infrastruktúra

FIGYELJÜK MEG …

- Az SaaS
  - szolgáltatás biztosítási (deployment/delivery) modell
    - Egy szolgáltató (vendor) adja az erőforrást (host) és a menedzsmentet
    - Interneten keresztül
  - üzleti modell: felhasználás (use, transaction, storage) szerinti
- Architektúrájában: „társbérleti” (multi tenancy), skálázható, biztonságos

felhasználónál	Felhasználónál (hosted)	IaaS	PaaS	SaaS
alkalmazás	alkalmazás	alkalmazás	alkalmazás	alkalmazás
VM	VM	VM	szolgáltatás	szolgáltatás
szerver	szerver	szerver	szerver	szerver
tároló	tároló	tároló	tároló	tároló
hálózat	hálózat	hálózat	hálózat	hálózat

Ellenőrzés a felhasználónál

A felhasználó megosztja az ellenőrzést a szolgáltatóval

Szolgáltatói ellenőrzés

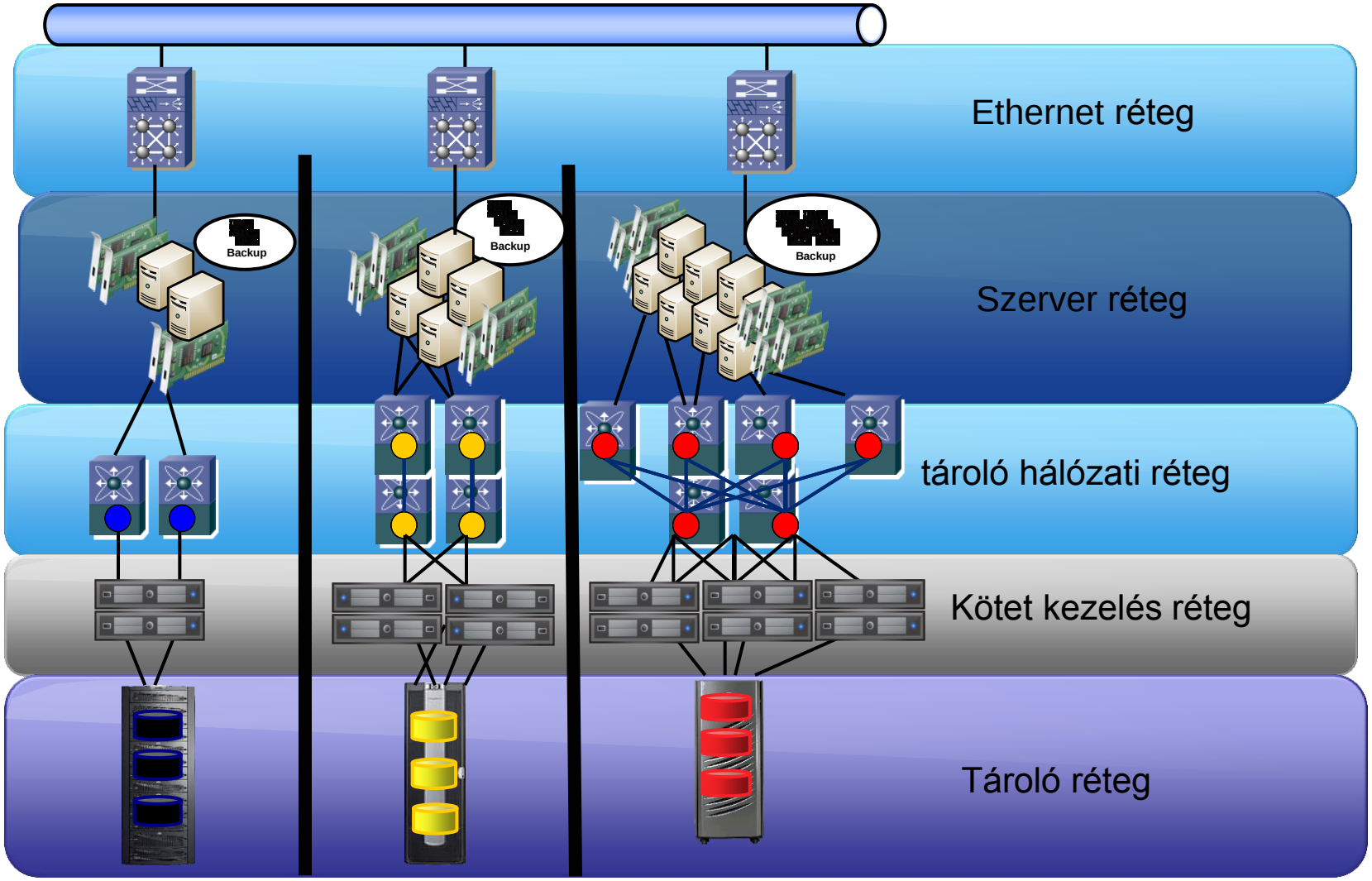
A VALÓS FORGATÓKÖNYVEK ENNÉL VÁLTOZATOSABBAK LEHETNEK

- Nyilvános felhő
- Magánfelhő
- A nyilvános felhő egy része a felhasználó telephelyén, az ottani tűzfal mögött is lehet
  - ezen belül: Iaas, Paas, SaaS szintű szolgáltatás
  - + külön szolgáltatások
- …
- Ezek eltérő üzemeltetési megoldásokat igényelnek.

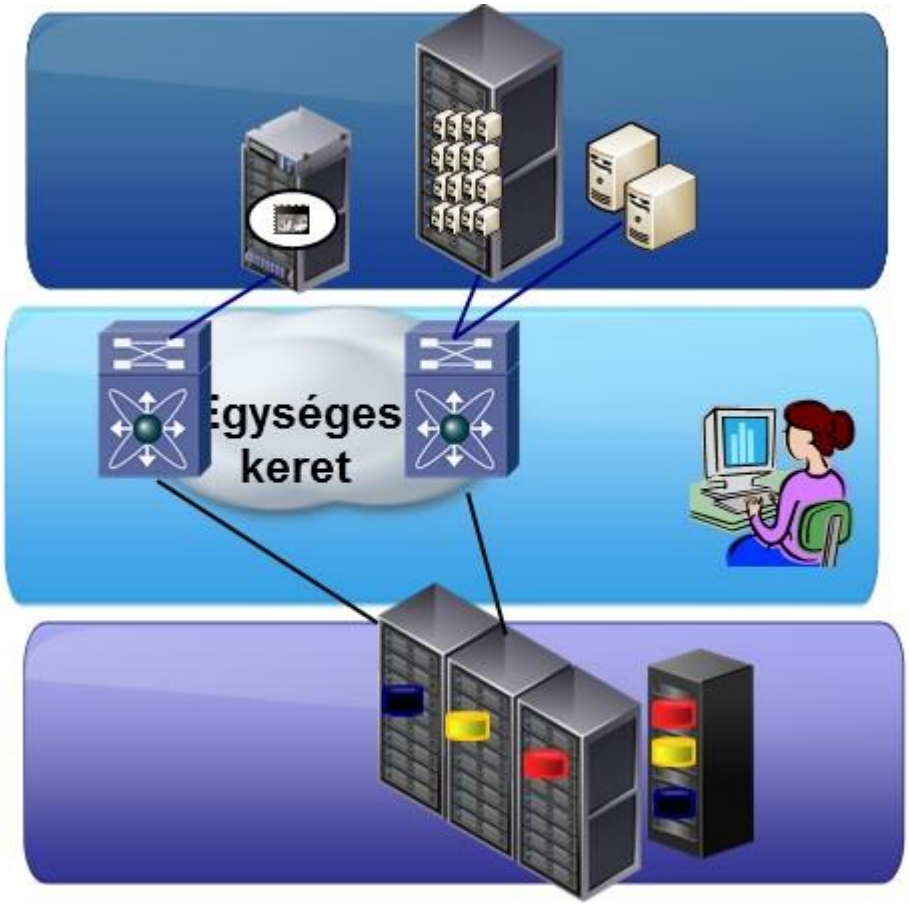
MIGRÁCIÓ A FELHŐBE?

- Miért?
  - költségtakarékosság
  - energiatakarékosság
  - „zöld IT”
  - nagyobb fürgeség a szoftver piacon
  - biztonsági megfontolások
- Hogyan?
  - áttelepülés nyilvános felhő IT-be
  - magánfelhő létrehozása
    - adatközpont migrálása magánfelhővé
    - új magánfelhő IT
  - hibrid migráció
    - fontos: az adat- és alkalmazás-hordozhatóság megoldása

MIGRÁCIÓ: A KIINDULÁS



MIGRÁCIÓ UTÁN



EGYÜTTMŰKÖDTETHETŐSÉG (INTEROPERABILITY)

A felhő IT-k együttműködtethetősége szabványosítást kíván.

- adat- és alkalmazás-hordozhatóság
- felhő IT-k integrálhatósága

De: a túlspecifikáltság megölné az innovációt.

EGYÜTTMŰKÖDTETHETŐ MODULOK EGY SZOLGÁLTATÁS-ALAPÚ KÖRNYEZETBEN

EGYÉNI FELHASZNÁLÓ:
- Internet
- Blog/Twitter/Web
- Info/tudásmegosztás (pl. wiki)
- Közösségi háló

SZERVEZETI VÉGFELHASZNÁLÓ:
- kommunikáció (e-mail, chat, IM)
- Együttműködés (csoportmunka)
- Munkaeszközök (szövegszerkesztő, táblázatkezelő, stb.)

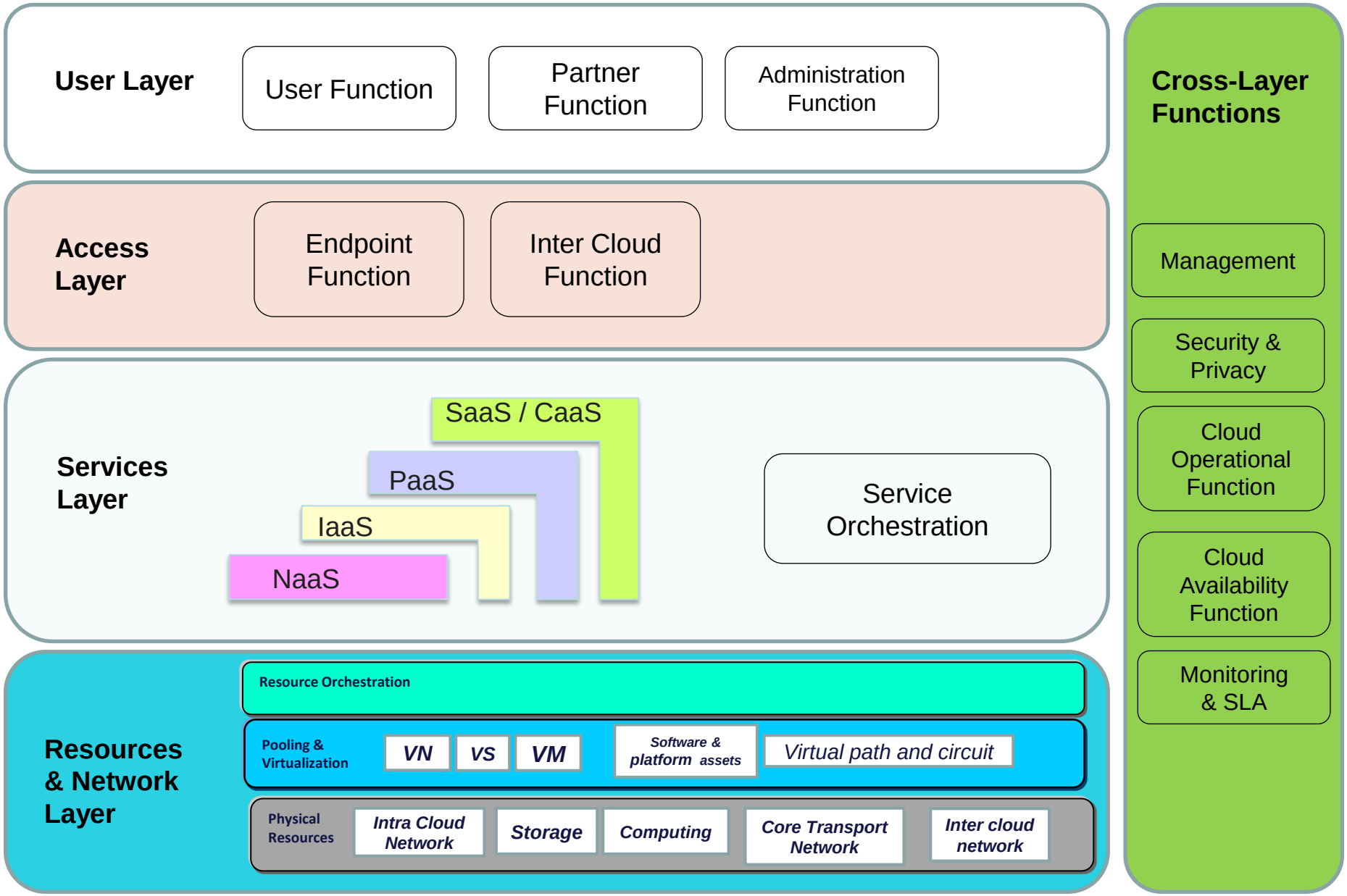
MENEDZSMENT SZOLGÁLTATÁSOK:
- biztonság
- azonosítás
- Cloud Menedzsment
- Service Level Agreement (SLA)

SZERVEZETI SZOLG. (SaaS):
- Kormányzati Apps
- Fizetési szolgáltatások
- Utazási szolgáltatások

ÜZLETI SZOLGÁLTATÁSOK (SaaS):
- HR, FM, költségvetés, stb.
- Supply Chain Management, ERP

PLATFORM SZOLGÁLTATÁSOK (PaaS):
- directory, autentikáció, autorizáció, stb.
- adatbázis menedzsment, munkafolyamat automatizáció, ütemezés,
- alkalmazás fejlesztés, tesztelés, minőségbiztosítás

INFRASTRUKTÚRA SZOLGÁLTATÁSOK (IaaS):
- Szerver/számítási erőforrás-bérlés (hosting)
- tárolás
- IT hálózati szolgáltatások
- Távközlő alapszolgáltatások


User Layer
User Function
Partner Function
Administration Function
Access Layer
Endpoint Function
Inter Cloud Function
Services Layer
SaaS / CaaS
PaaS
IaaS
NaaS
Service Orchestration
Resources & Network Layer
Resource Orchestration
Pooling & Virtualization
VN
VS
VM
Software & platform assets
Virtual path and circuit
Physical Resources
Intra Cloud Network
Storage
Computing
Core Transport Network
Inter cloud network
Cross-Layer Functions
Management
Security & Privacy
Cloud Operational Function
Cloud Availability Function
Monitoring & SLA

SZABVÁNYOSÍTÁSI TÖREKVÉSEK

- UCI: Unified Cloud Interface by Cloud Computing Interoperability Forum (CCIF).
  - http://groups.google.com/group/unifiedcloud
- OCCI: The Open Cloud Computing Interface by Open Grid Forum (OGF).
  - http://www.occi-wg.org

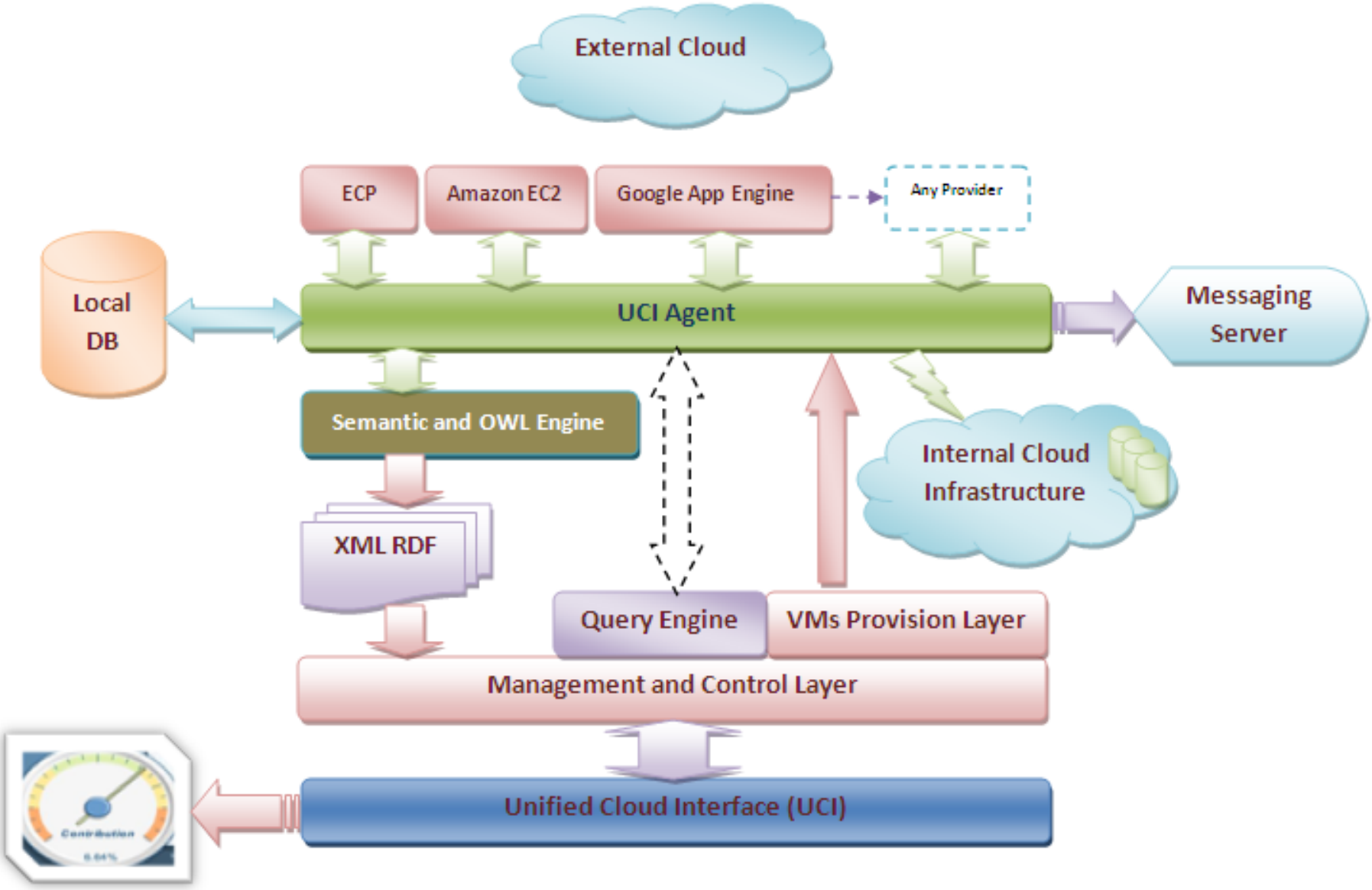
Lásd: Cloud Standards Wiki (cloud-standards.org)

Továbbá …:

- *ITU-T Focus Group on Cloud Computing*
- *OGF (Open Grid Forum)*
- *Cloud Computing Interoperability Forum*
- *NIST (National Institute of Standards and Technology)*
- *ETSI (European Telecommunications Standards Institute)*
- *OASIS (Organization for the Advancement of Structured Information Standards)*
- *DMTF (Distributed Management Task Force)*

UCI

- Az egységes felhő interfész (unified cloud interface = UCI) más néven „felhő bróker” egy szemantikus specifikációból és egy ontológiából áll (Semantic Cloud Abstraction). Az ontológia tartalmazza az aktuális modell leírását, a specifikáció definiálja a más modellekkel való integrálás részleteit.
  http://groups.google.com/group/unifiedcloud



Forrás: http://code.google.com/p/unifiedcloud/

OCCI

OCCI = Open Cloud Computing Interface

- Az Open Grid Forum fejleszt egy specifikáció-készletet.
  Lényegében: protokoll és API különböző felhő IT menedzsment feladatokhoz.
  Eredetileg egy távoli (remote) menedzsment *„API for IaaS model based Services”* volt a cél (különböző felhő IT infrastruktúrákban közös feladatokhoz: szolgáltatás bevezetése, skálázása, monitorozása).
  Ebből egy rugalmas API nőtt ki: integráció, hordozhatóság, interoperabilitás céljaira (bővíthető).

OCCI SPECIFIKÁCIÓ

- kapcsolat
  - Single OCCI REST end point over HTTP(S).
- autentikáció
  - SSL/TLS, NTLM, Kerberos
- reprezentáció
  - OCCI deszkriptor formátum (alkalmazás/occi+xml)
  - nyílt virtualizációs formátum (alkalmazás/ovf+xml)
  - nyílt virtualizációs archívum (alkalmazás/x-ova)
  - konzol (VNC)

OCCI SPECIFIKÁCIÓ

- Deszkriptorok
  - feldolgozó (Compute)
  - hálózat (Network)
  - tároló (Storage)
- Azonosítók
  - URI-val hivatkozott erőforrások

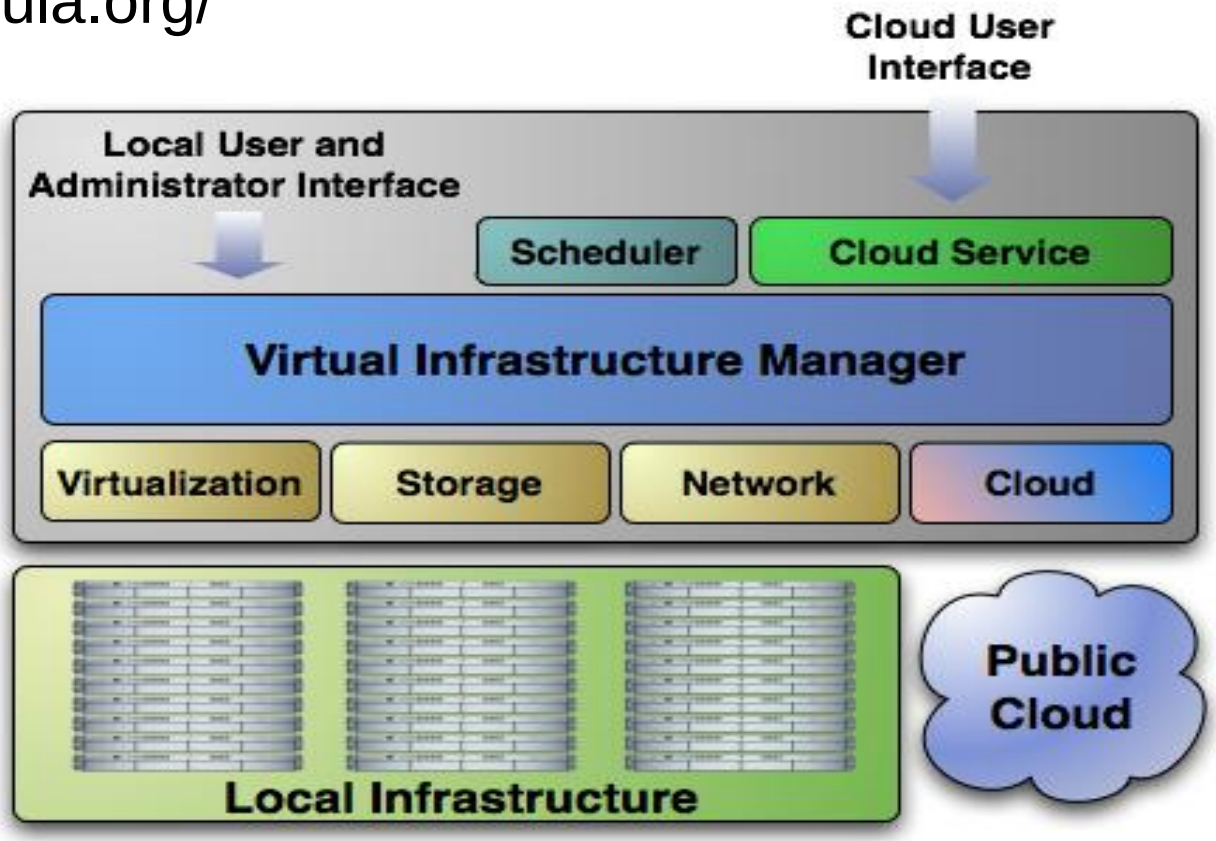
OCCI MŰVELETEK

- Create
  - POST
- Retrieve
  - GET
- Update
  - GET and PUT
- Delete
  - DELETE
- Requests
  - Trigger State Changes via POST

OCCI: OpenNebula

OpenNebula.org
The Open Source Solution for Data Center Virtualization

- nyílt forrású ipari standard adatközpont virtualizációhoz
- virtualizációs menedzsment eszköz
- http://opennebula.org/



NÉHÁNY MEGFONTOLÁS …

… pay-per-use alapú hozzáférés az Internet „*végtelen*” erőforrásaihoz
… az Internet NEM VÉGTELEN ERŐFORRÁS
… a „pay-per-use” jellemzően keveredik egy „fix” komponenssel (előfizetés vs. pre-paid)

… a felhő infrastruktúra ad keretet az alkalmazásokhoz való skálázható, megbízható, igény szerinti hozzáféréshez …
… mindennek ára van: ez új infrastruktúra réteget jelent

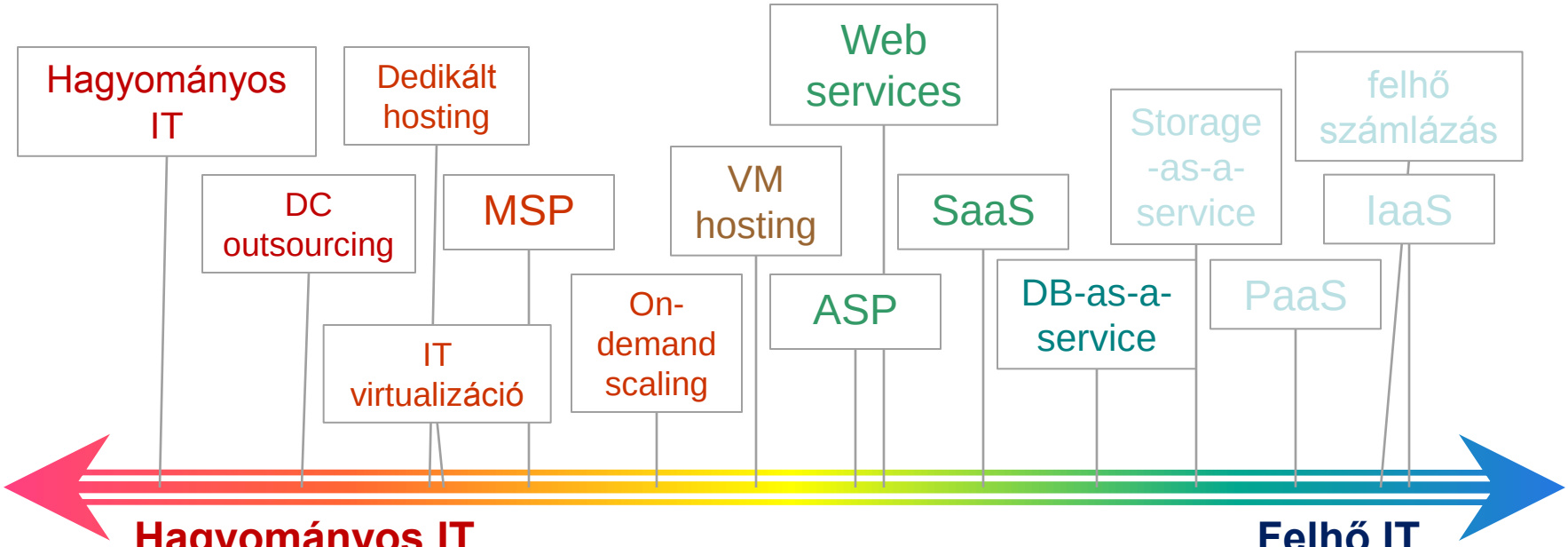
… a felhő szolgáltatások „láthatatlan” hátteret (backend) adnak a legtöbb mobil alkalmazáshoz is …
… mégis van néhány nagy elkülönült platform

… nagyfokú rugalmasság ez energiafogyasztásban …
… csak „nagyban” értelmes

… a földrajzi elhelyezkedés nem számít
… bizalom, jogi szabályozás, stb. – sokszor számít

- Felhő operációs rendszer: az adatközpontok erőforrás-együttesekként kezelhetők (pools of resources) – a szerver virtualizáció új fázisa
- Menedzsment réteg: felügyelet, automatizálás, hatékony erőforrás allokáció
- Önkiszolgáló portálok operátorok, sys admin-ok és felhasználók számára
- standard API-k „cloud-aware” alkalmazásokhoz

NEM MEGY MINDEN A FELHŐBE



Hagyományos IT
- fix költség/feltételek
- változó bevezetés
- egyetlen felhasználó
- több „kézivezérlés”
- testreszabhatóság

Felhő IT
- változó költség/feltételek
- standard bevezetés
- „társbérlet”
- nagyon automatizált
- korlátozott testreszabhatóság

Autonóm adatbázis

Autonóm adattárház

Autonóm infrastruktúra …

… az admin elfogja veszíteni a munkáját ?

Változó karrierpálya:

- Rutinfeladatok automatizálása
  - Szabály, profil, mesterséges intelligencia
  - Gyorsabban, olcsóbban, kevesebb hibával
- Új technológiák bevezetése (verziók, új termékek)
- Heterogén környezet kialakítása, fenntartása
- DevOps részvétel

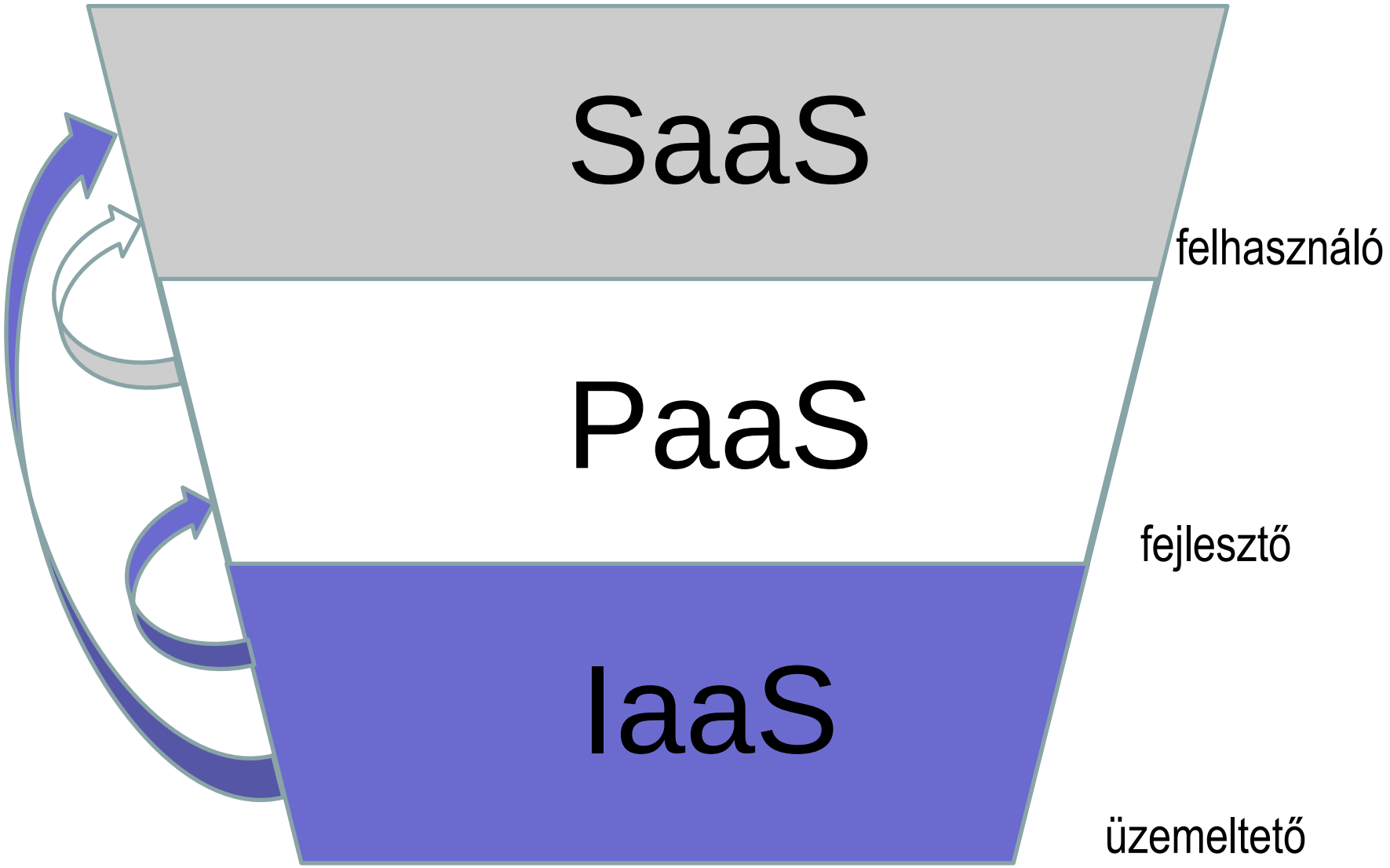
II. RÉSZ

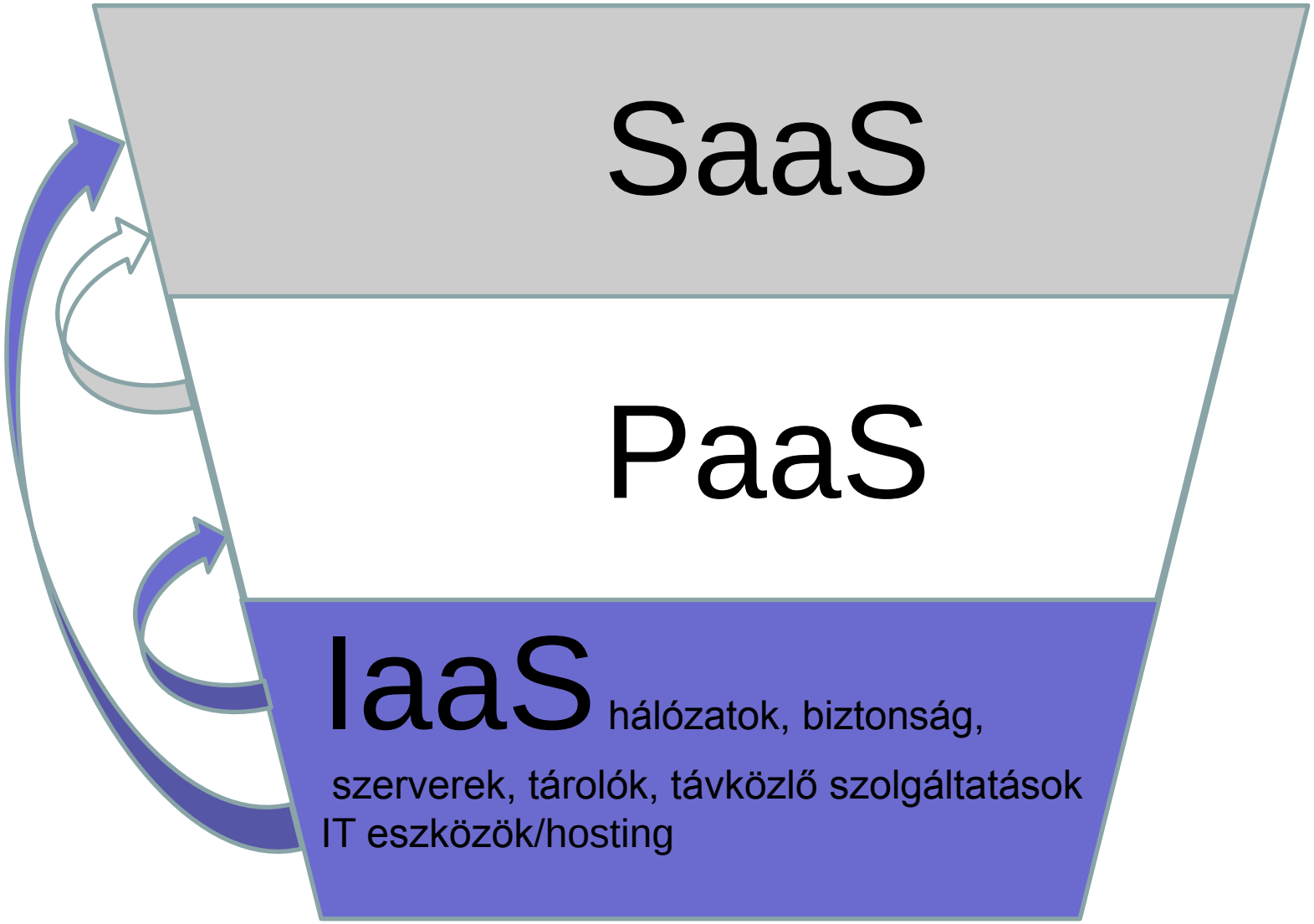
VIRTUALIZÁCIÓ, FELHŐ
OTTHONI FELDOLGOZÁSRA

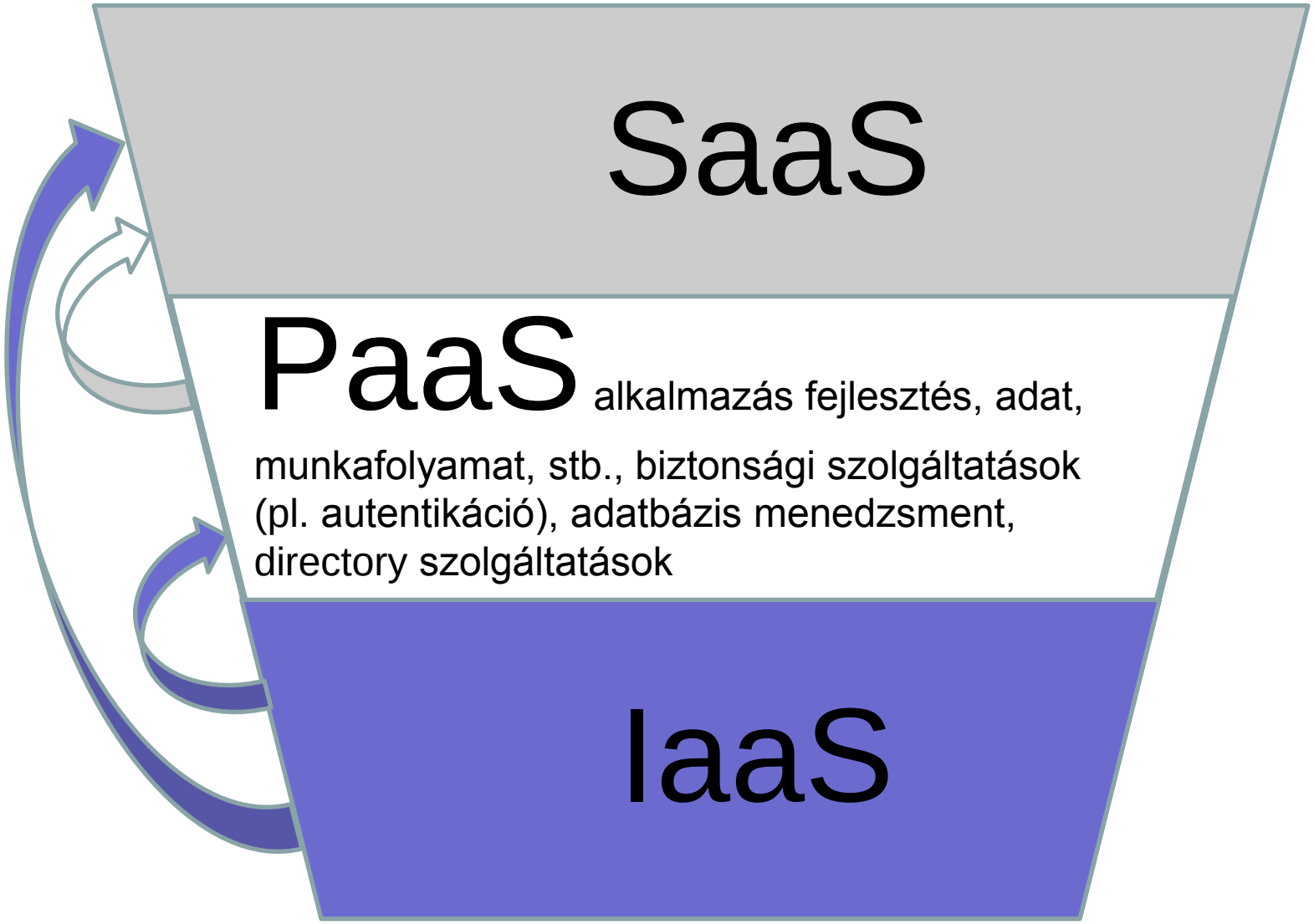
SaaS (Software as a Service): szoftver szolgáltatási modell, amiben a felhasználó alkalmazás licencet kap, igény-szerinti (on demand) szolgáltatásként

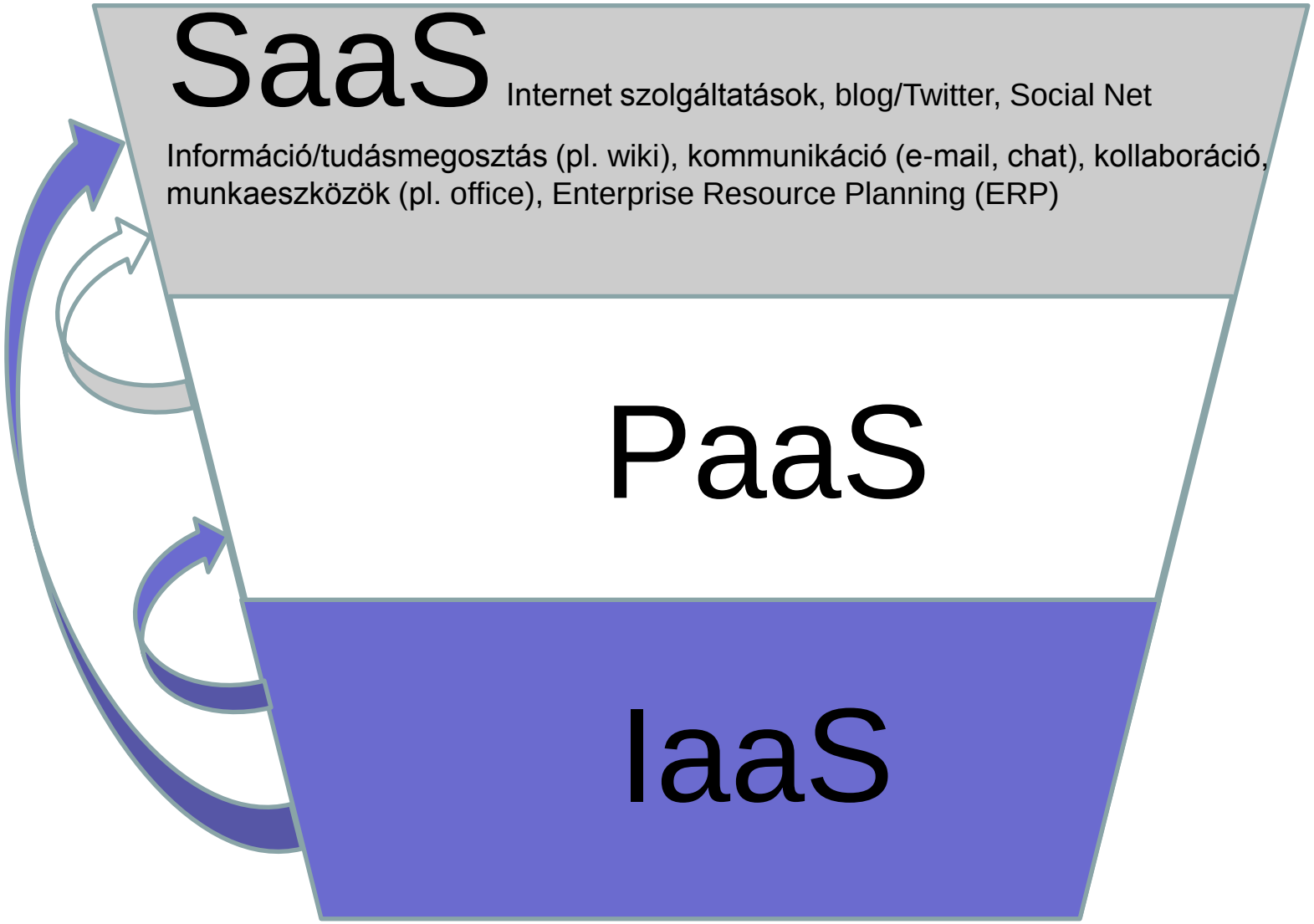
PaaS (Platform as a service): IT platform & megoldási csomag szolgáltatásként

IaaS (Infrastructure as a Service): IT infrastruktúra, mint szolgáltatás (tipikusan platform virtualizációs környezet)


SaaS
felhasználó
PaaS
fejlesztő
IaaS
üzemeltető


SaaS
PaaS
IaaS hálózatok, biztonság,
szerverek, tárolók, távközlő szolgáltatások
IT eszközök/hosting


SaaS
PaaS alkalmazás fejlesztés, adat,
munkafolyamat, stb., biztonsági szolgáltatások
(pl. autentikáció), adatbázis menedzsment,
directory szolgáltatások
IaaS


SaaS
Internet szolgáltatások, blog/Twitter, Social Net
Információ/tudásmegosztás (pl. wiki), kommunikáció (e-mail, chat), kollaboráció, munkaeszközök (pl. office), Enterprise Resource Planning (ERP)
PaaS
IaaS

SaaS (Software as a Service): szoftver szolgáltatási modell, amiben a felhasználó alkalmazás licencet kap, igény-szerinti (on demand) szolgáltatásként

PaaS (Platform as a service): IT platform & megoldási csomag szolgáltatásként

IaaS (Infrastructure as a Service): IT infrastruktúra, mint szolgáltatás (tipikusan platform virtualizációs környezet)

Típusai

- Nyilvános felhő (Public Cloud)
- Magánfelhő (Private Cloud)
- Hibrid felhő (Hybrid Cloud)

TÍPUSAI

- Nyilvános felhő (Public Cloud)
  - az IT infrastruktúrát egy szolgáltató a saját telephelyein működteti. Az ügyfél nem tudja, nem befolyásolja, hogy hol. Az infrastruktúrán tetszőleges ügyfelek osztoznak.
- Magánfelhő (Private Cloud)
- Hibrid felhő (Hybrid Cloud)

TÍPUSAI

- Nyilvános felhő (Public Cloud)
- Magánfelhő (Private Cloud)
  - dedikált IT infrastruktúra egy bizonyos szervezet számára, nem osztozik mással *(… lehet, hogy ez nem is igazi felhő IT ???)*; drágább, biztonságosabb, mint a nyilvános felhő IT
  - *on-premise* (az adott szervezet telephelyén) vagy *externally hosted* (egy felhőből dedikálva)
- Hibrid felhő (Hybrid Cloud)

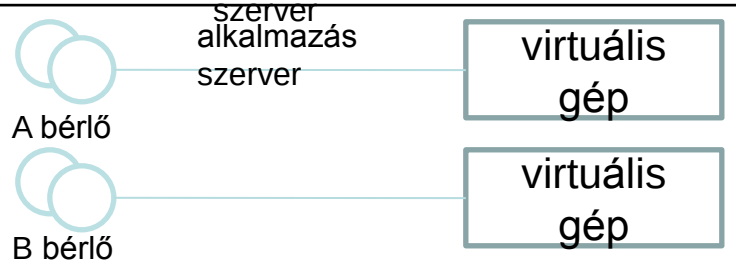
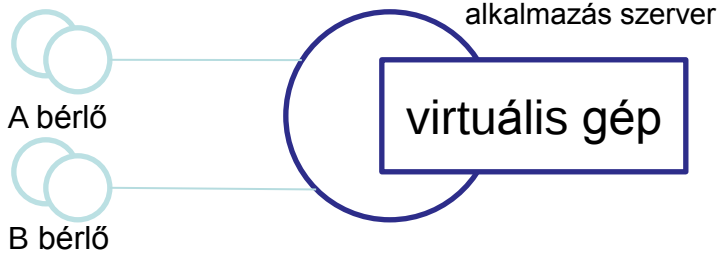
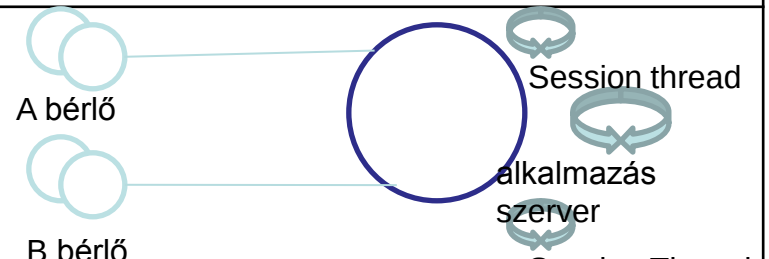
TÍPUSAI

- Nyilvános felhő (Public Cloud)
- Magánfelhő (Private Cloud)
- Hibrid felhő (Hybrid Cloud)
  - pl. (1) kritikus alkalmazások magánfelhőben, mások nyilvános felhőben;
    pl. (2) normál IT üzem a szervezet saját infrastruktúráján, különleges/csúcs terheléshez pótlólagos erőforrás nyilvános felhőből

TÁRSBÉRLET (MULTI TENANCY)

- A szoftver egy példánya a szolgáltató infrastruktúráján fut
- Több bérlő férhet hozzá ugyanahhoz a példányhoz
- A több felhasználós (multi-user) modelltől eltérően a társbérlet egy adott példány testre szabását igényli (a különböző bérlők igényei szerint)
- A társbérleti alkalmazásnál a bérlők ugyanazon a hardver erőforráson osztoznak, amit megosztott alkalmazás és adatbázis példány használ, de úgy, hogy azok konfigurálhatók (mintha dedikált lenne)
- Mit is jelent ez?
  - Az alkalmazások osztozhatnak a hardver erőforrásokon.
  - A szoftver konfigurálható.
  - Egyetlen alkalmazás és DB példányt több bérlő használhat

TÁRSBÉRLETI MÓDOK ALKALMAZÁS SZERVERHEZ

Izolált alkalmazás szerver Mindegyik bérlő alkalmazás szerverhez fér, amelyik dedikált szervereken fut.	
Virtualizált alkalmazás szerver Mindegyik bérlő dedikált alkalmazáshoz fér, amelyik szeparált VM-en fut.	
Osztott virtuális szerver Mindegyik bérlő dedikált alkalmazás szerverhez fér, amelyik osztott VM-en fut.	
Osztott alkalmazás szerver A bérlő az osztott alkalmazás szerveren az alkalmazást szeparált szálon (thread) / session-ön keresztül éri el.	

SaaS – ÜZEMELTETÉS SZEMPONTJÁBÓL

megjelenítés

- Menü, navigáció
- UI vezérlők
- Megjelenítés, rendering
- Riport

biztonság

- szövetségi jogosultság
- „Single Sign on”
- autorizáció, szerep-alapú hozzáférés
- jogosultság
- titkosítás
- szabályosság

alkalmazás

- User Profile
- előfizetések
- metaadat vezérelt lépések
- metaadat szolgáltatások
- üzenetkezelés
- munkafolyamat
- végrehajtás kezelés
- orchestration
- adat-szinkronizálás

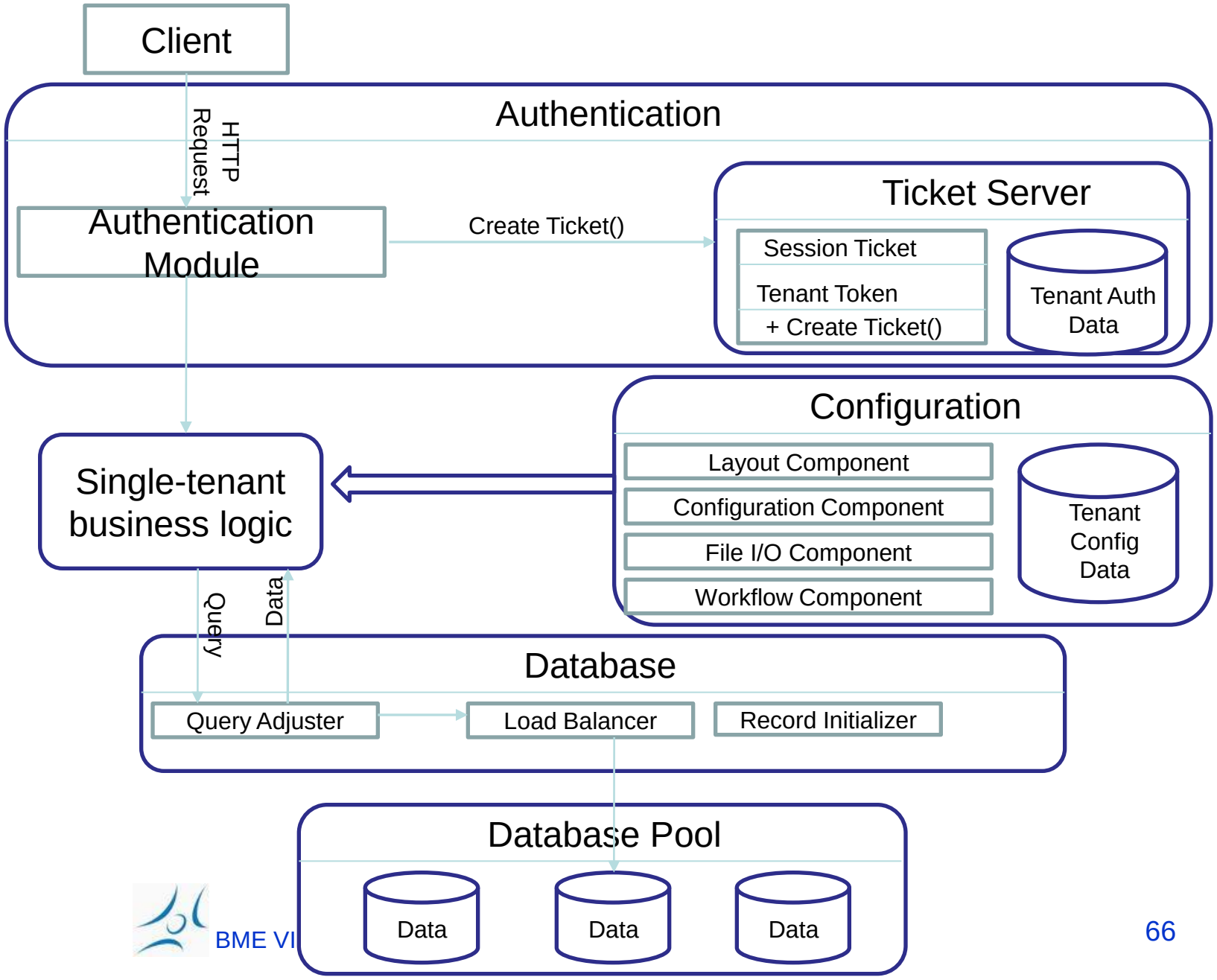
működtetés

- Monitoring
- Backup and Restore
- tartalékolás
- konfiguráció testreszabás
- teljesítmény
- mérések

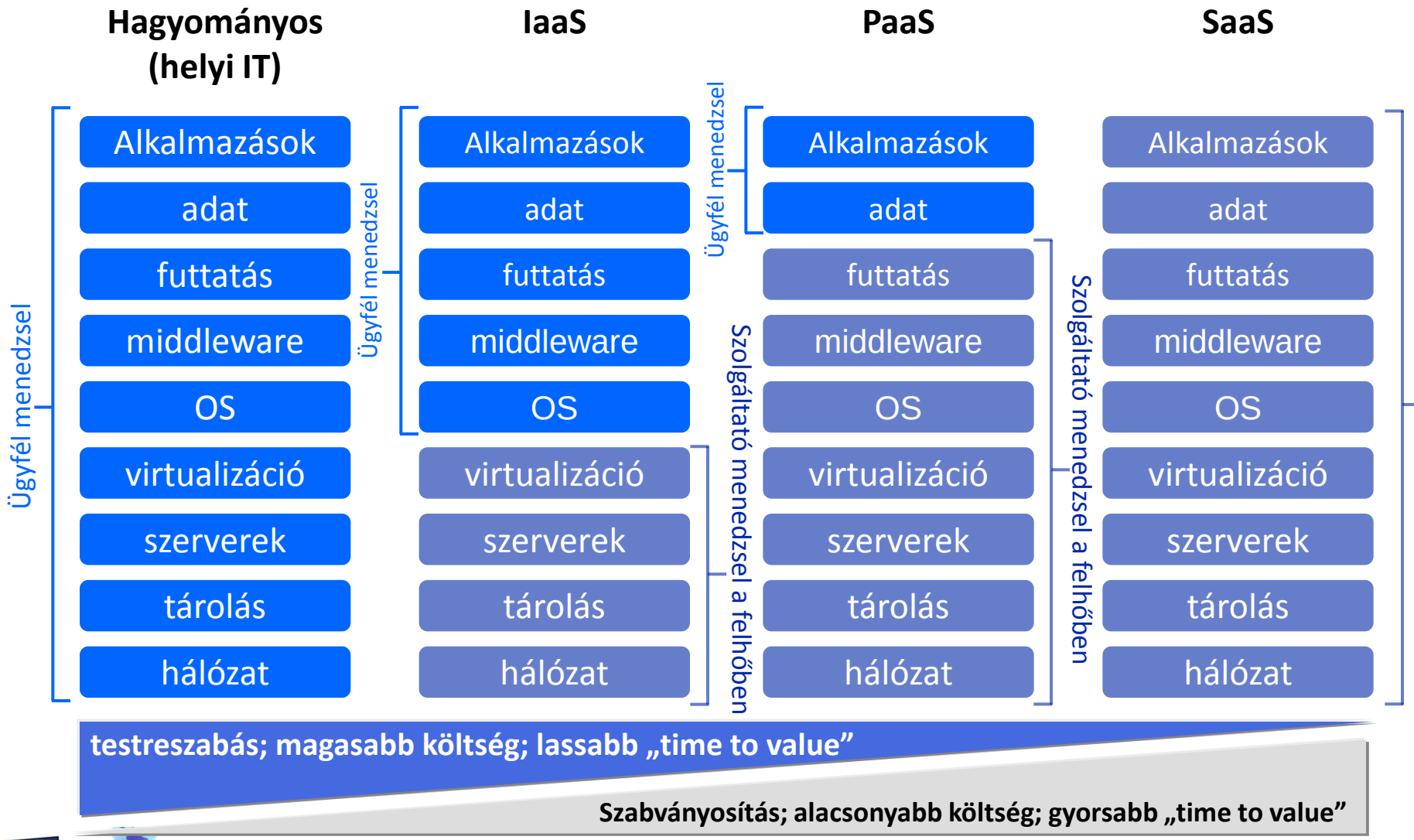
Infrastruktúra

- DB
- tárolás
- számítógép
- hálózat

TÁRSBÉRLETI ARCHITEKTÚRA PÉLDA



AZ ÜZLETI IGÉNYBŐL KELL KIINDULNI



A FELHŐ IT BIZTONSÁGI ELŐNYEI

- Egységes biztonsági politika.
- Automatizált biztonsági eljárások és műszaki megoldások.
- A felhő homogenitása egyszerűbbé teszi az ellenőrzést és az auditálást.
- Redundancia, mentés/helyreállítás.

A FELHŐ IT BIZTONSÁGI ELŐNYEI

- Dedikált biztonsági szakértelem.
- Technológiai naprakészség.
- Nagy(obb) befektetés a biztonsági infrastruktúrába.
- Hibatűrés és megbízhatóság tervezése.
- Valós idejű támadás-észlelés.
- Kapcsolódás biztonsági kezdeményezésekhez.

A FELHŐ IT BIZTONSÁGI KOCKÁZATAI

Felhő IT = komoly erőforrás koncentráció

== komoly kockázat-koncentráció

- egy átfogó hiba következményei kiterjedtebbek lehetnek
- az ügyfelek koncentrációja egyúttal veszélyeztetettség-koncentrációt is jelent

Általában: elosztott rendszerekben nem elegendő csak a jelszó/tanúsítvány autentikáció + az adatátvitel bizalmasságának megőrzése.

- Pl. egy felhő IT specifikus támadás *„csendes”* lehet, nem feltétlenül hagy nyomot az adott node operációs rendszerében.

NEM LESZ NAGY BAJ, HA …

- a felhő szolgáltató biztonsági politikája legalább olyan erős, mint az ügyfél elvárása,
- a felhő szolgáltató szakemberei jók, felelősségteljesek,
- a web-service interfészek nem hoznak be túl sok sebezhetőséget,
- …

LEHETSÉGES PROBLÉMÁK

- tipikus:
  - az ellenőrzés elvesztése
  - bizalomhiány (mechanizmus !)
  - sok bérlő-társ
- A fentiek a nyilvános felhő IT-re vonatkoznak.

AZ ELLENŐRZÉS ELVESZTÉSE

- A felhasználó a szolgáltatóra bízza
  - adatbiztonság, privacy, erőforrás-elérhetőség, monitoring és javítás/helyreállítás
- Az ügyfél elveszítheti az ellenőrzést
  - adatai, alkalmazásai, erőforrásai felett, amelyek (fizikailag) a szolgáltatónál vannak
  - a felhasználók (személy)azonosítása felett
  - a felhasználói hozzáférési szabályok érvényesítése felett

INTÉZKEDÉSEK ELLENŐRZÉS MEGTARTÁSÁHOZ

- monitoring
- különböző felhők használata
- hozzáférés menedzsment

MONITORING

- Az ügyfél-igény pontos azonosítása
  - Mi a teendő egy bizonyos hiba esetén?
  - Visszaállítási mechanizmus (mi a szolgáltató és mi az ügyfél dolga ?)
- Alkalmazás-specifikus run-time monitoring és menedzsment eszköz
  - Az ügyfél is kaphat hozzáférést az eszközhöz
  - Szolgáltató/ügyfél: eltérő nézetek
  - Az ügyfél is beavatkozhat?
    RAdAC (Risk-adaptable Access Control); VM remote portolás másik fizikai host-ra, jog és lehetőség másik felhőbe átmozgatni az alkalmazást

HOZZÁFÉRÉS-SZABÁLYOZÁS (ACCESS CONTROL)

- Különböző szintek (pl. hozzáférés a felhőhöz, szerverhez, szolgáltatáshoz, adatbázishoz: közvetlenül/ web services, VM-hez, VM objektumhoz
- Ügyfél-menedzselt hozzáférés
- Autentikáció: végső soron a szolgáltató biztosítja

BIZALOMHIÁNY

- Definiálni kell a kockázatokat és a bizalmi kérdéseket
  - Különböző érdekei vannak a szolgáltatónak és az ügyfélnek!
  - Ne csak akkor merüljön föl, ha már megtörtént a baj.
- Menedzsment sémák
  - Egyensúlyozni a bizalom és a kockázat között

A SOK BÉRLŐ-TÁRS KÉRDÉSE

- Konfliktusok lehetősége a bérlők érdekkülönbözőségei miatt
  - minden lehetséges esetre jó együttműködési szabály-rendszer nincs,
  - ha valaki nem „fair” játékos, mit lehet kezdeni vele?
- Egyáltalán: az ügyfelek elválasztásának kérdése is része a felhő üzemeltetési politikának.
  - erős/gyenge elválasztás
  - VPC: az erőforrások azért végesek és megosztottak

POLICY LANGUAGE

- Standard SLA nyelvezet
  - Géppel értelmezhető (feldolgozható),
  - Kombinálható/összehasonlítható leíró blokkok
  - “a VM-ek elválasztása szükséges”, “a VM-ek fizikai elválasztása szükséges”, stb.
  - Validációs eszköz: az üzemeltetési politika az SLA-ban a létrehozó szándékait tükrözi-e?

A BIZALOMVESZTÉS ELKERÜLÉSE: TANÚSÍTVÁNYOK

- Tanúsítvány (Certification):
  - elismert, független, ellenőrizhető leírása a biztonsági kérdéseknek és a biztosításnak
- Kockázatértékelés
  - third party
  - biztosítási konstrukció alapja is lehet