

Felhő alapú szolgáltatások - SaaS - és ami mögötte van

Előadó: Szabó Gábor
Director, Hospitality Business Unit

Felhő alapú szolgáltatások története

- 1950 es évek – óriási és drága számítógépek -> időmegosztás, eszközmegosztás
- 1960 as évek – ARPANET -> INTERNET
- 1970 es évek – IBM virtuális gépek megjelenése
- 1990 es évek – Internet forradalom
- 2000 es évek – Multinacioális cégek elkezdtek Felhő alapú szolgáltatást ajánlani ügyfeleiknek

Felhő definíció (NIST - National Institute of Standards and Technology)

A felhő alapú szolgáltatás az egy olyan informatikai szolgáltatási modell, amely lehetővé teszi azt hogy bárhol, kényelmesen, igény szerint nyújtson hálózaton keresztül hozzáférést megosztott számítástechnikai erőforrásokhoz, amelyeket gyorsan rendelkezésre lehet bocsátani úgy, hogy nagyon kevés adminisztratív tevékenységre és minimális szolgáltatói interakcióra van esetleg szükség.

Felhő definíció (NIST - National Institute of Standards and Technology)

- A felhő alapú szolgáltatásoknak 5 alapvető jellemzője kell legyen:
 - Igény szerinti önkiszolgálás
 - Széleskörű hozzáférhetőség
 - Helyszíntől független erőforrás készlet
 - Teljes rugalmasság
 - Mérhető szolgáltatási mennyiség

Felhő típusok

Nyilvános felhő



- Klasszikus felhő: szolgáltatások és infrastruktúra megosztása több ügyféllel
- Önkiszolgáló, interneten keresztül elérhető
- Biztonsági, irányítási és felügyeleti kérdések

Magán felhő



- 1 ügyfélnek biztosít infrastruktúrát és szolgáltatást
- Több felügyelet és irányítási lehetőség az ügyfélnek
- Drágább mint a nyilvános felhő

Közösségi felhő



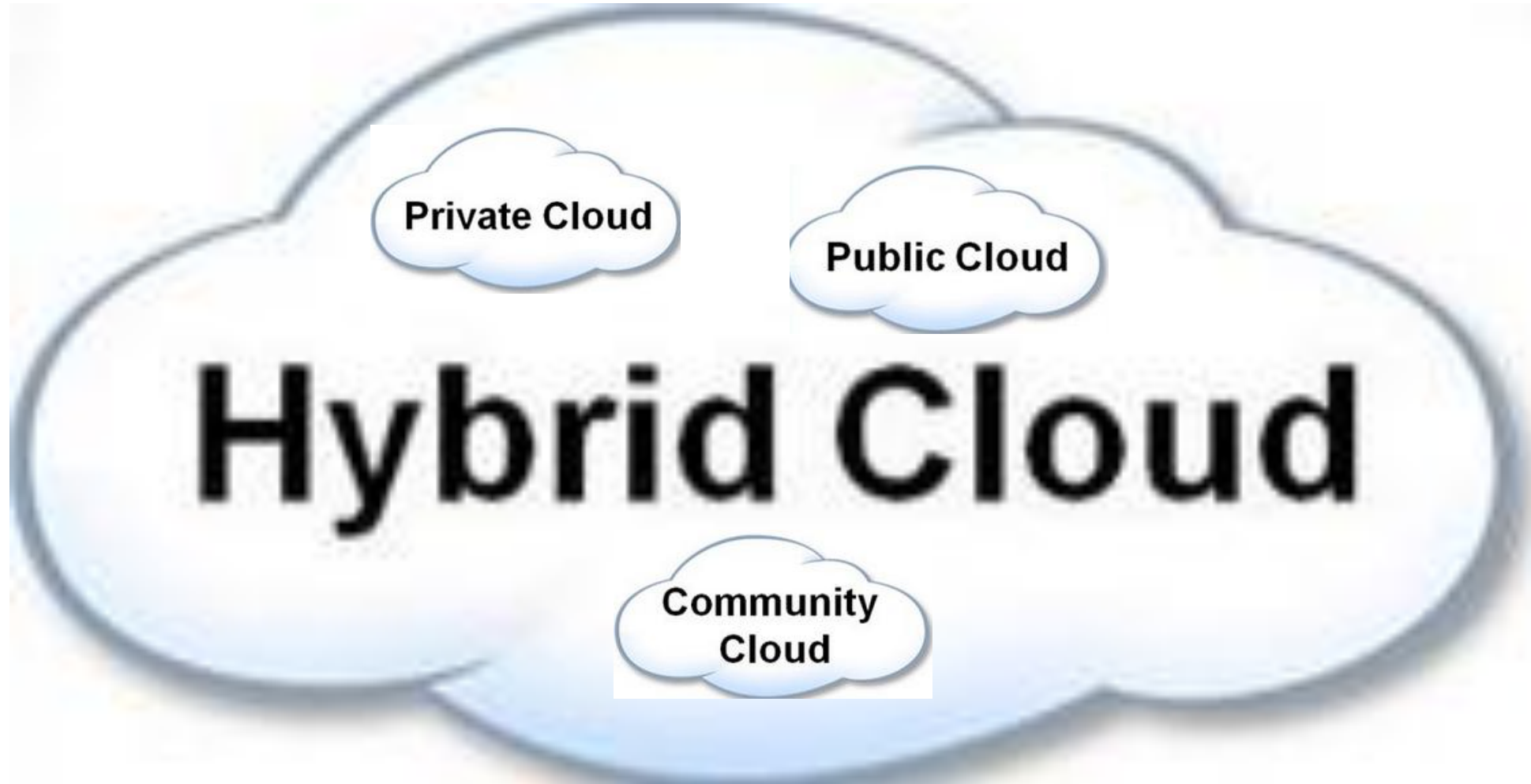
- Azonos tevékenységet folytató szervezetek között megosztott
- Egy közös cél
- Költségmegosztás

Hibrid felhő

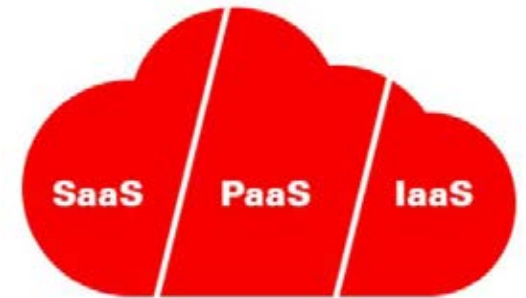


- Felhőtípusok kombinációja
- Bonyolultabb – biztonsági kérdések mikor nyilvános és magán felhőt kombinálunk akár több felhőszolgáltató is szerepet játszhat
- Skálázható, költséghatékony, átjárható

Felhő típusok



Felhő alapú szolgáltatások



- **Infrastrukturális számítási felhő (infrastructure as a service):** az ügyfelek számára hálózatot, tárhelyet, és minden olyan erőforrást biztosít a szolgáltató ami ahhoz kell, hogy a saját Operációs rendszerét, szoftvereit fejleszteni és futtatni tudja. Az ügyfél nem ismeri a felhő infrastruktúrát, viszont ő felel és felügyeli az operációs rendszert, a tárhely kapacitást, az alkalmazást is néhány hálózati komponenst is., mint például a tűzfalat.
- **Platform alapú számítási felhő (platform as a pervice):** az ügyfél számára a szolgáltató biztosítja a lehetőséget, hogy a saját alkalmazását fejleszthesse, futtathassa a szolgáltató által a rendelkezésére bocsájtott eszközökkel. Ezáltal a felhasználó nem látja és nem felügyeli az infrastruktúrát (tárhely, Operációs rendszer, hálózat) csak és kizárólag a saját alkalmazását és maximum néhány háttér beállítást
- **Szoftver alapú számítási felhő (software as a service):** a szolgáltató lehetőséget nyújt az ügyfeleinek, hogy használja a szolgáltató alkalmazásait, amik elérhetőek különböző eszközökről, különböző módokon. Az ügyfél nem látja a felhő infrastruktúrát, még az alkalmazás architektúrát sem, csak talán néhány alkalmazáson belüli beállítást.
- Egyéb:
 - Database as a Service (DBaaS)
 - Storage as a Service (STaaS)
 - Hardware as a Service (HWaaS)

Felhő evolúció



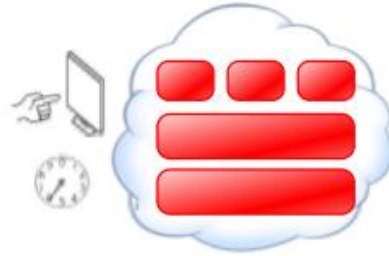
Tradicionális

- Fizikai szerverek
- Dedikált rendszerek
- Heterogén rendszerek



Konszolidált

- Virtuális szerverek
- Megosztott rendszerek
- Standardizált rendszerek



Magán felhő

- Igény szerinti önkiszolgálás
- Automatikus erőforrás hozzárendelés
- Mérhetőség



Nyilvános felhő

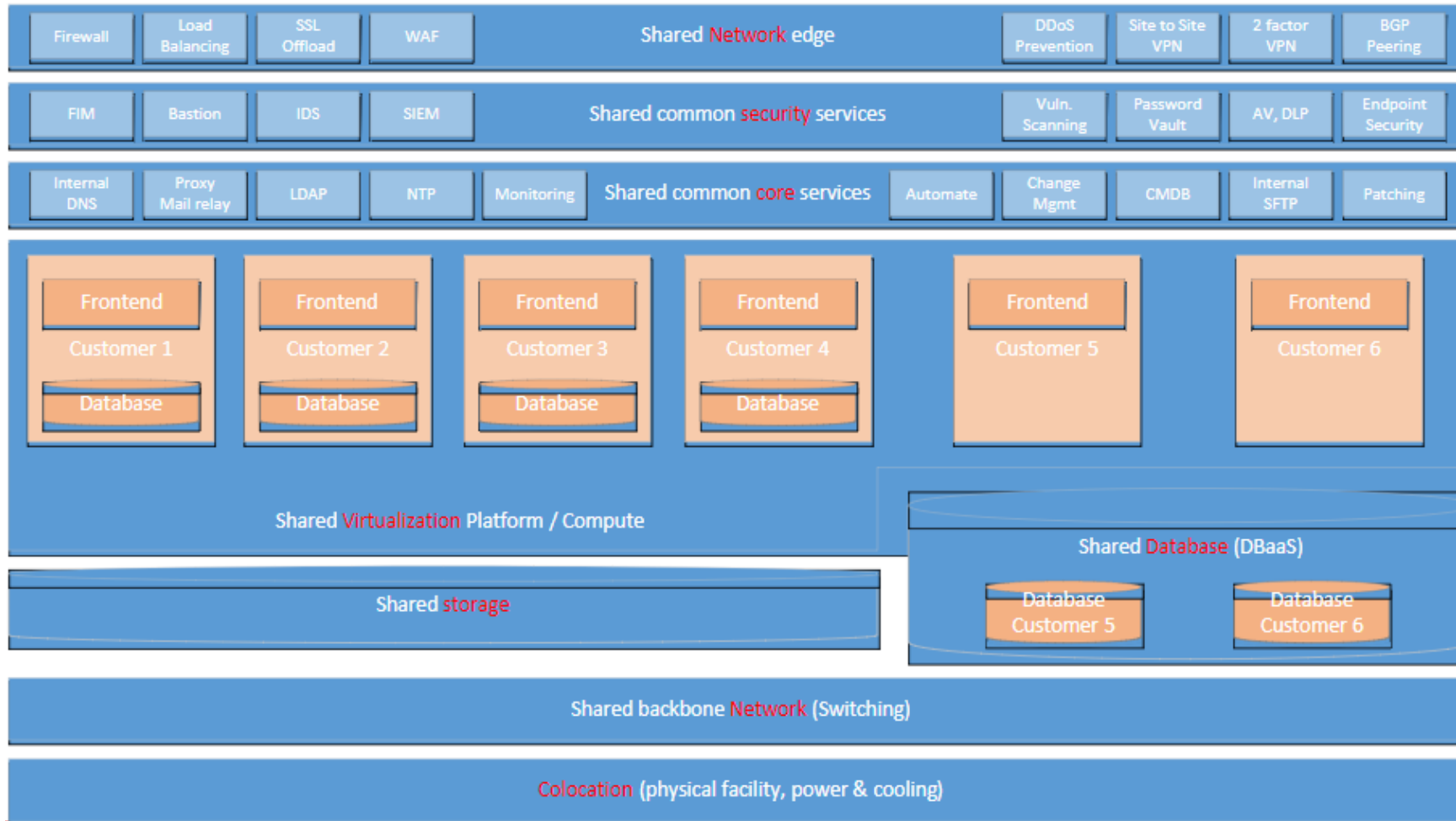
- Specializálhatóság alkalmazás szinten
- Megosztott rendszerek
- Standardizált platform



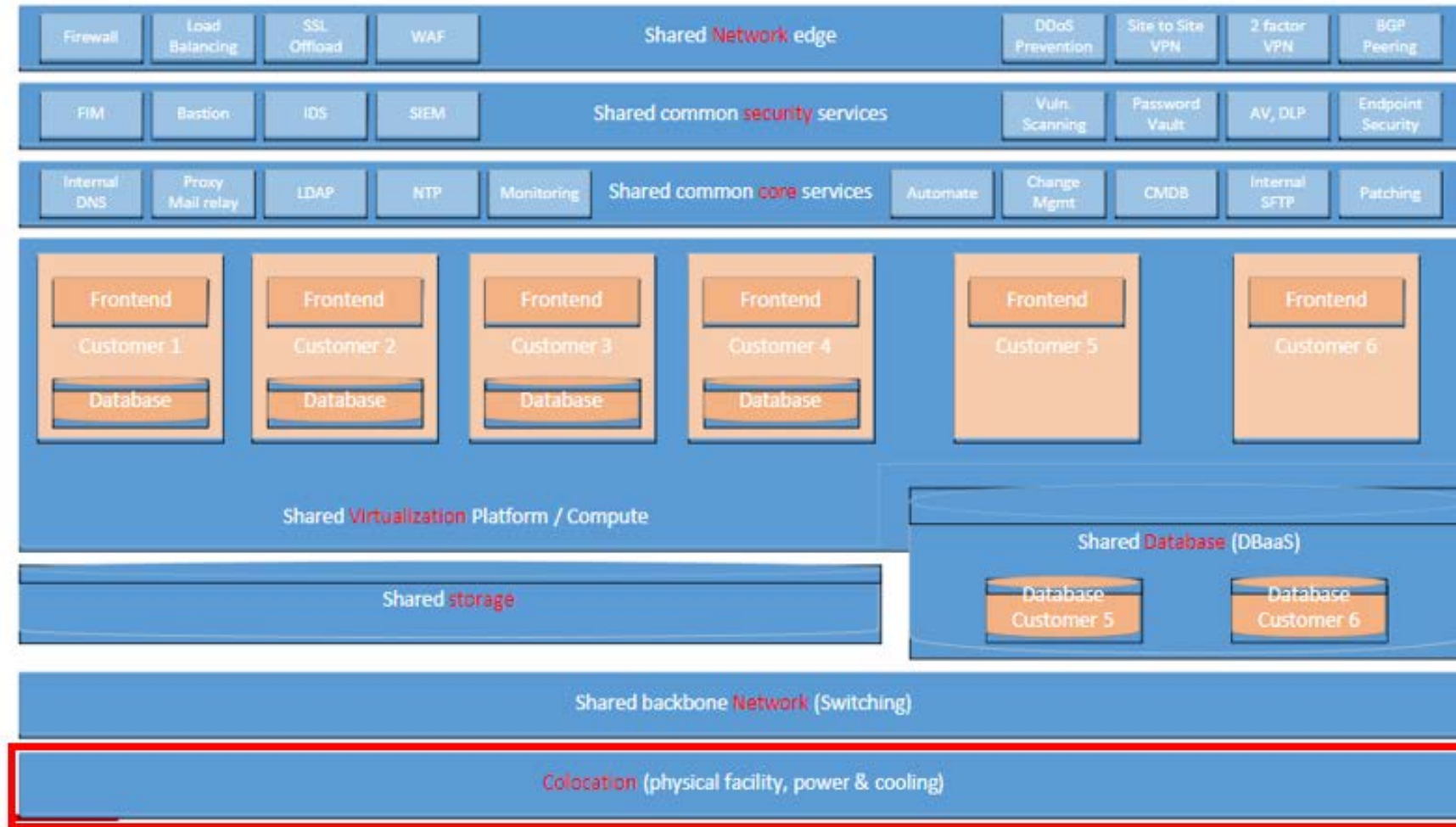
Hibrid felhő

- Nyilvános és magán felhő együtt, azok minden előnyét kihasználva

Felhő és ami mögötte van - felépítés



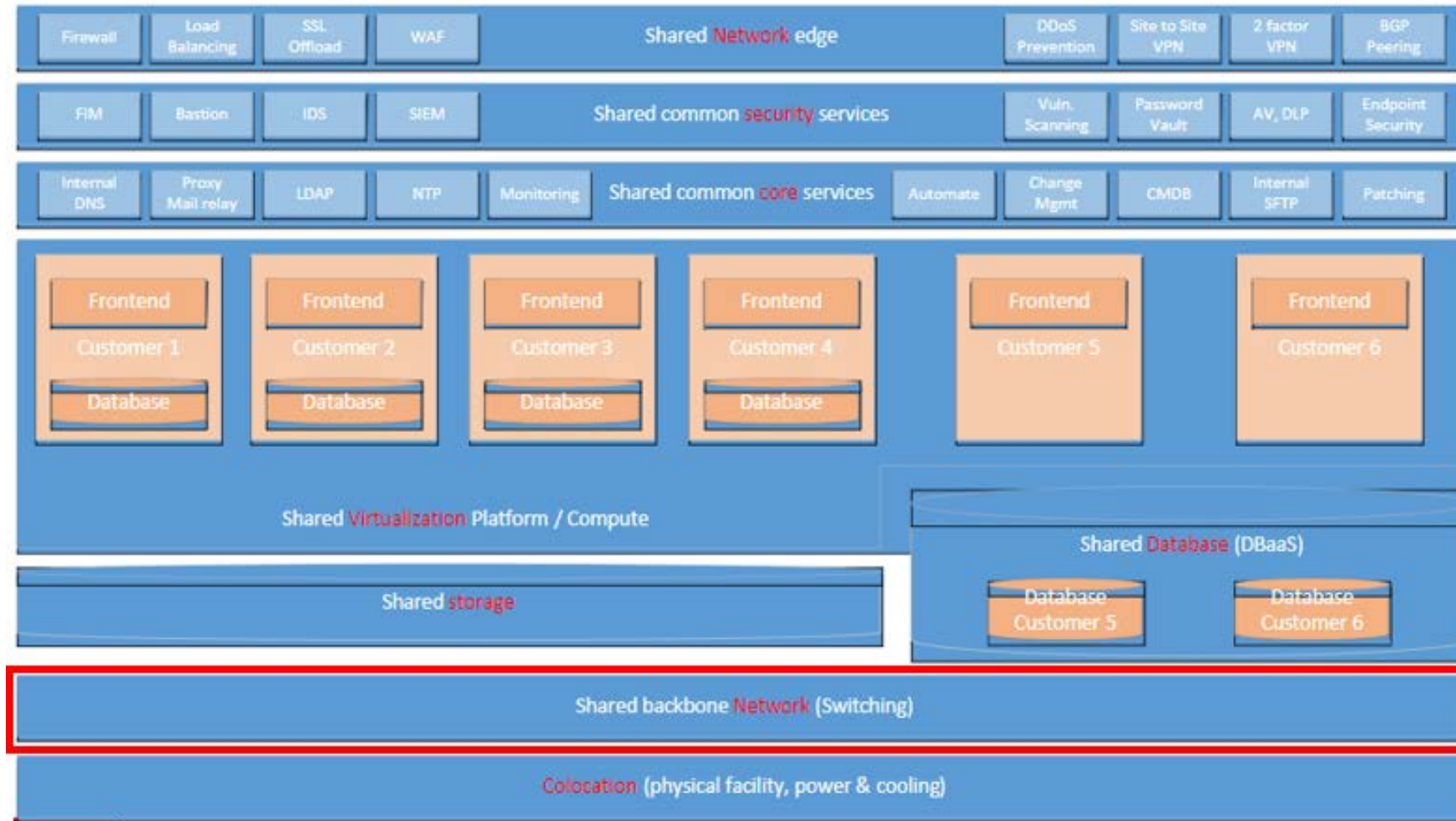
Felhő és ami mögötte van



Felhő és ami mögötte van – Fizikai infrastruktúra

- Fizikai hozzáférés és biztonság
- Tűzvédelmi rendszer
- Hőmérséklet és páratartalom monitoring:
 - Állandó hőmérséklet: $22\text{ C}^{\circ} \pm 2\text{ C}^{\circ}$
 - Állandó páratartalom: $50\% \pm 15\%$
- Redundáns áramszolgáltatás mellett:
 - UPS - szünetmentes tápegységek
 - Legalább 10 percig üzemképes akkumlátorok
 - Generátorok
 - Legalább 72 órára elég üzemanyag a generátorokhoz
 - Áramellátás monitoring

Felhő és ami mögötte van



Felhő és ami mögötte van – Hálózat



- Redundáns:
 - Routerek
 - Switchek
 - Tűzfalak
 - Load balancerek
 - Behatolás érzékelő hálózati eszközök

Felhő és ami mögötte van

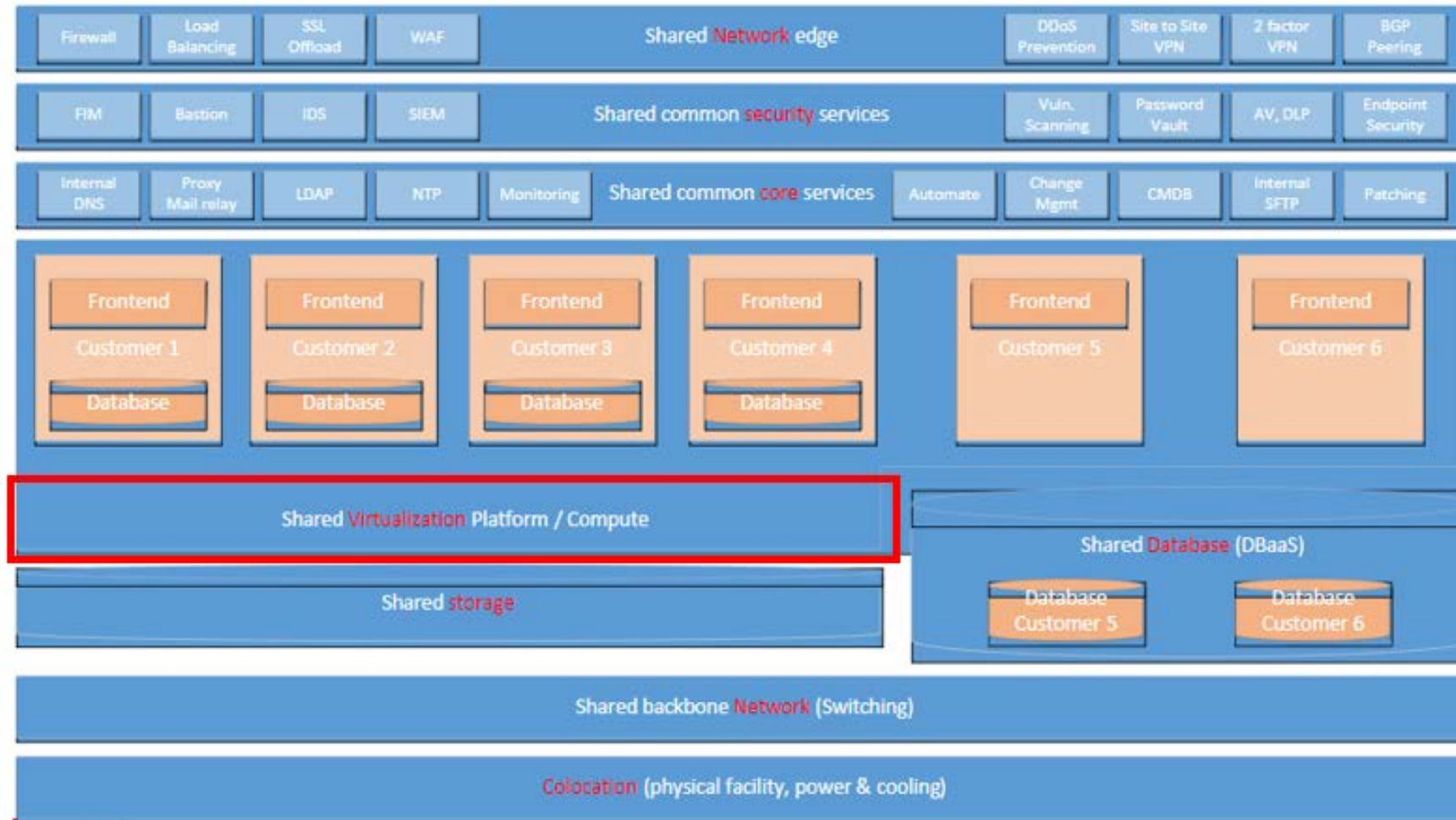


Felhő és ami mögötte van – Tárhely



- High Capacity
 - Nagyon sok tárhely kapacitás
 - Kevesebb redundancia
 - Lassabb elérés
 - Általában test rendszerek, nem kritikus rendszerek, mentések tárolására
- High availability
 - Rendkívül gyors elérés
 - Magas szintű redundancia – zero data loss
 - Kevesebb tárhely kapacitás
 - Éles rendszerrel adataira

Felhő és ami mögötte van



Felhő és ami mögötte van – Fizikai szerverek



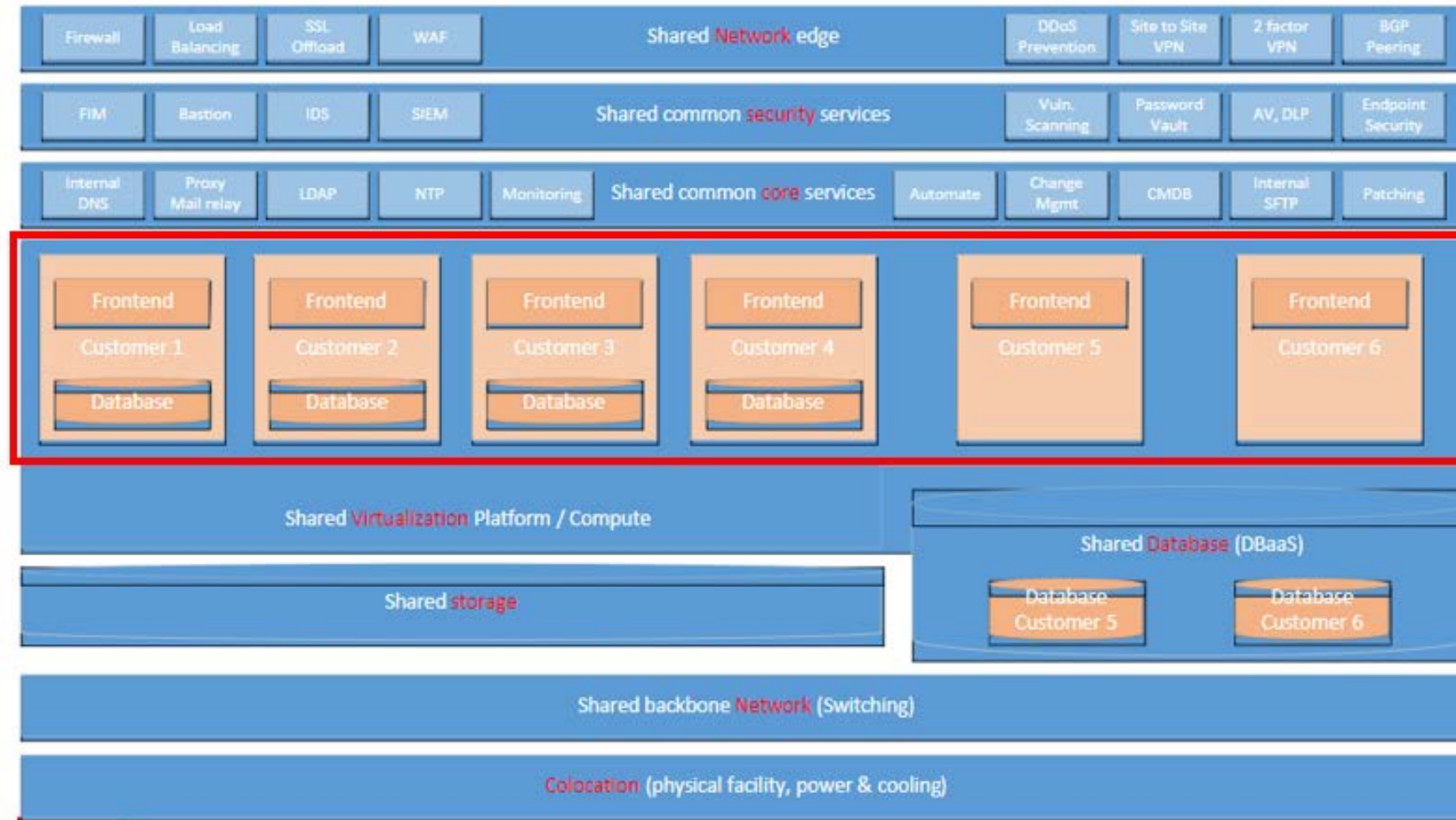
- Rendkívül nagy teljesítményű számítógépek
- Redundáns, legalább 2 tápegység
- Redundáns, legalább 2 hálózati kártya
- Ezek az alapjai a virtualizációnak
- Ezek adják az ugynevezett compute kapacitást:
 - Memória – akár 8TB
 - CPU – akár 512 CPU core

Felhő és ami mögötte van – Speciális hardware – EXADATA



- Arra lett kitalálva, hogy minél gyorsabb fusson rajta az Oracle adatbázis.
- Gyakorlatilag hardware szinten értelmezi az SQL utasításokat
- All in ONE adatbázis monstrum:
 - 4 TB DRAM
 - 22TB flash – akár 220TB tömörített adat – Összes aktív adat memóriában
 - 8 magos Intel Xeon E5-2690 processzorok
 - Akér 1.5 millió disk olvasás 1 mp alatt
 - 500TB tárhely
 - Íráskor is a flash cache-t használja, így akár 1 millió írást is tud mpként
 - Oracle Enterprise linux
 - Oracle 12c adatbázis
 - 40X10Gb port

Felhő és ami mögötte van



Felhő és ami mögötte van – Virtualizáció



Hagyományos virtualizáció	Cloud virtualizáció
Virtuális gépek létrehozása kézzel történik, nincs automatikus lehetőség	Virtuális eszközök, gépek listája, ami lehetővé teszi hogy gyorsan és kockázat mentesen hozzunk létre virtuális eszközöket
Nincs dinamikus erőforrás kezelés	Pool erőforrások automatikus és dinamikus kezelése
Fix kapacitású tárhely, fix hálózat	Dinamikus szerver pool, rugalmas network, megosztott, rugalmas tárhely kapacitás
Különböző csapatok bejövő jegyek és kérések alapján hozzál létre a gépeket: Rendszer adminok telepítik az Operációs rendszert, Storage mérnökök hozzák létre a kapcsolódó tárhelyeket, hálózati mérnökök konfigurálják a hálózatot, stb.. Ez szekvenciális és időigényes	Automatizációnak köszönhetően a virtuális gépek létrehozása gyors, és egyszerű, nem igényel emberi beavatkozást csak akkor, ha az erőforrások kimerülőben vannak, illetve ha az ügyfélnek speciális igényei vannak

Cloud virtualizáció variánsok

- Hardware virtualizáció

Mindent virtualizálunk az OS-sel együtt. A virtuális gépben futó operációs rendszer ideális esetben nem is tud arról, hogy nem fizikai hardveren fut, hanem egy virtuális gépben.

- Docker konténeres virtualizáció:

A konténerek szervezése szolgáltatás alapon történik, minden szolgáltatásnak konténert, saját környezetet definiálunk, amelyek között a célszerűségnek megfelelően linkeket képzünk. A konténerek többszörözése szükség esetén könnyen megtehető, így egy adott szolgáltatást pillanatok alatt több példányban futtathatunk.

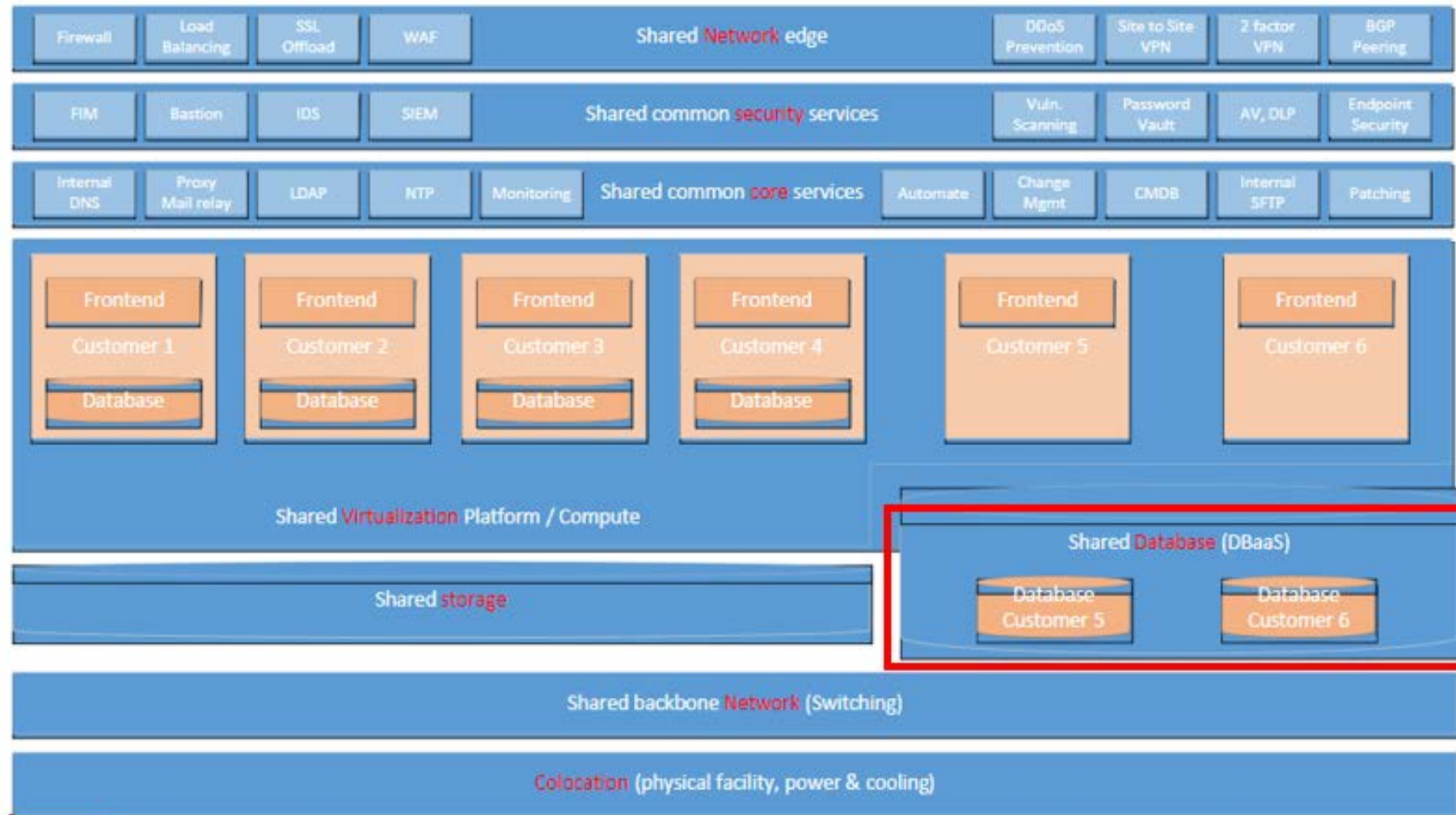
Docker
konténerek

Különböző
Hypervisorok

Különböző OS

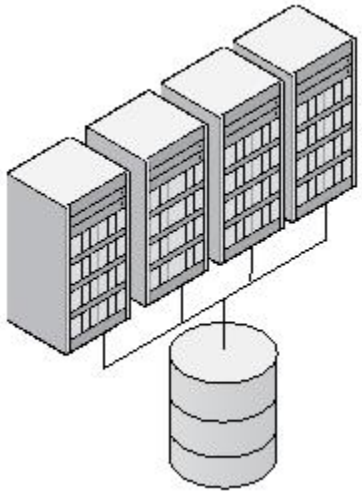


Felhő és ami mögötte van



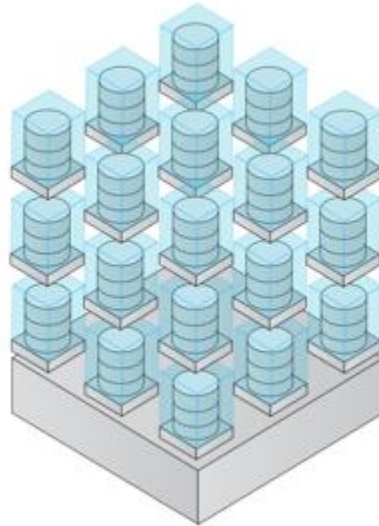
Oracle Cloud – Database as a Service - Evolúció

Virtuális gépek



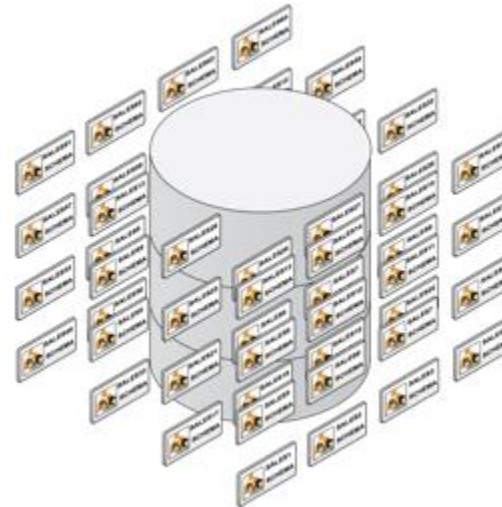
Megosztott hardware

Adatbázis példányok



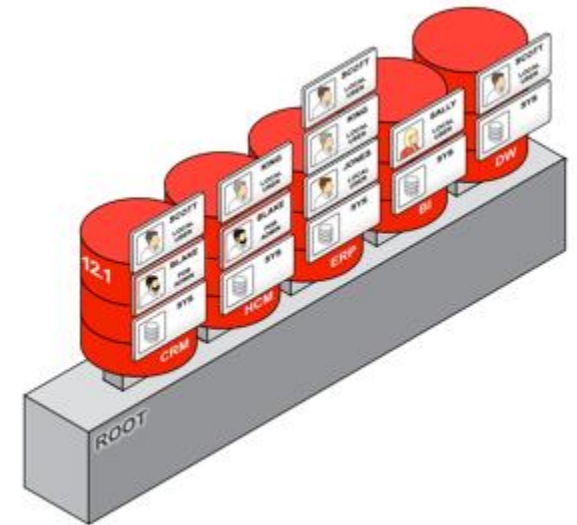
Megosztott hardware
és OS

Séma konszolidáció



Megosztott
hardware, OS és DB

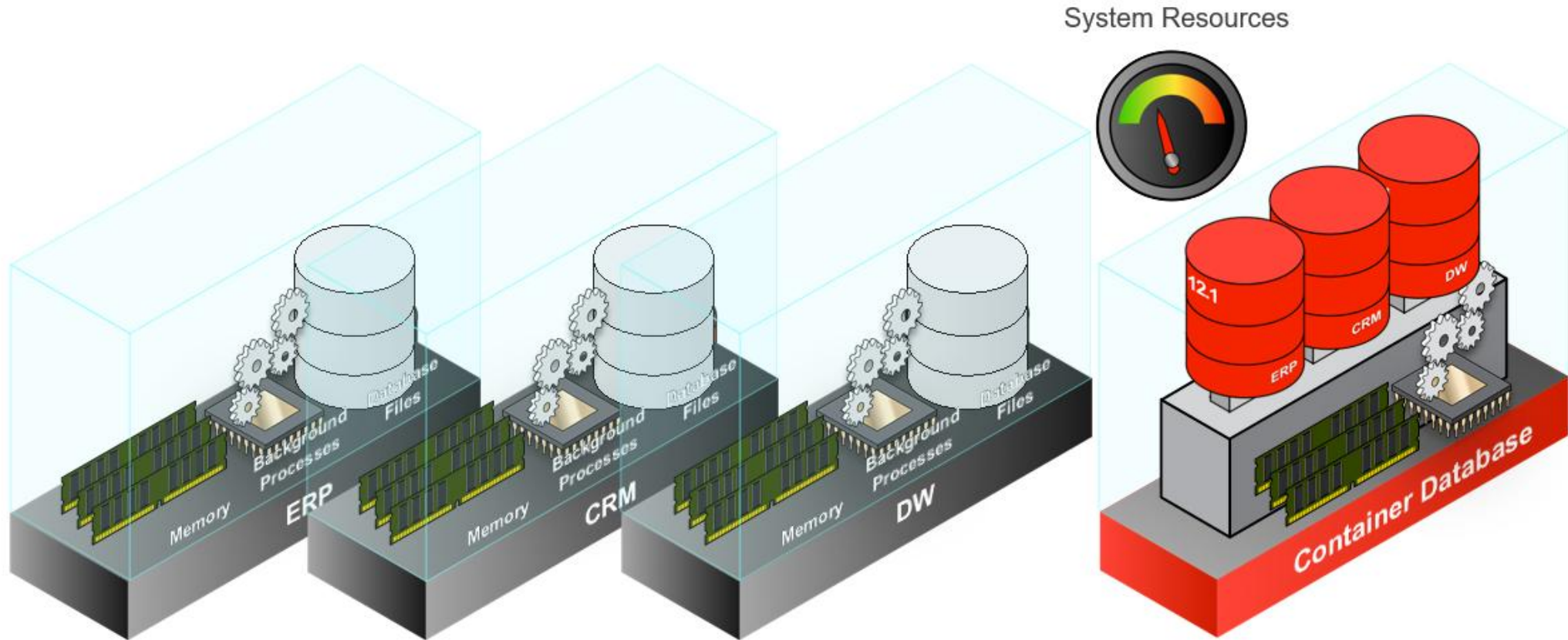
Konténer adatbázisok



Megosztott
hardware, OS és DB

EVOLÚCIÓ

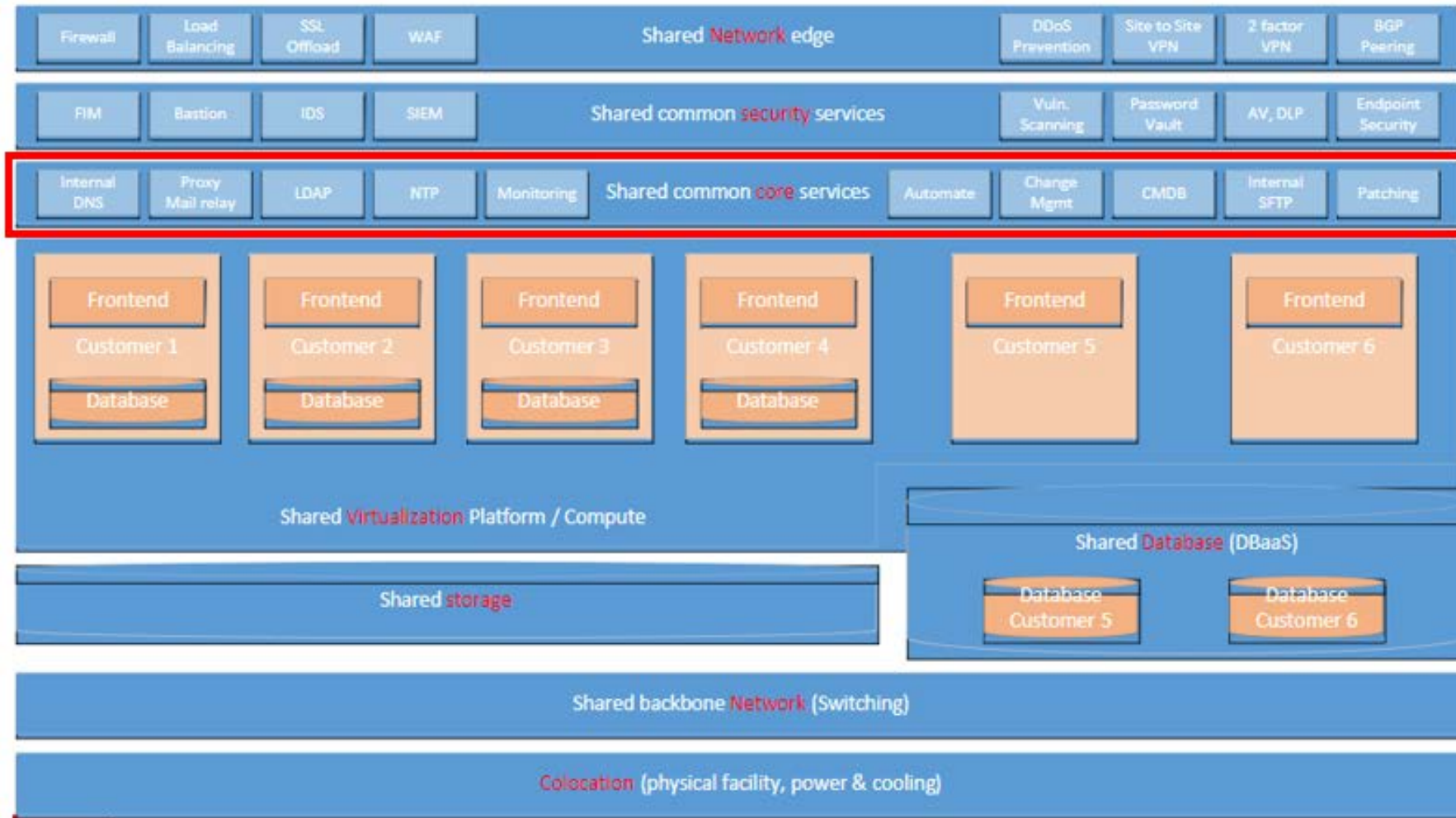
Oracle Cloud – Database as a Service - Evolúció



Felhő és ami mögötte van – Cloud adatbázisok – 12c

- Max 4096 PDB egy konténer adatbázisba – gyakorlatilag még egy igazán nagy vállalatnak is elég 1 konténer adatbázis az összes alkalmazásának futtatására
 - Isolalt, mégis multitenant
 - Sokkal hatékonyabb erőforráskezelés
 - Sokkal hatékonyabb karbantartás
 - Nem kell alkalmazás kódot változtatni, működik az alkalmazás továbbra is
- Erőforrás szabályozás CPU, I/O és memória szinten
- Sharding – adatbázisokat több szerver között el lehet osztani a párhuzamosítás, teljesítmény és megbízhatóság növelés érdekében
- Hot cloning – leállítást nélküli klónozás, migráció szerverek vagy éppen adatközpontok között
- Active Data Guardon is lehet lekérdezéseket futtatni – csökkentve a terhelést az éles rendszereken

Felhő és ami mögötte van



Felhő és ami mögötte van – Shared Core Services

- Internal DNS – belső és külső névfeloldás
- Mail servers – belső és külső levelezés
- LDAP – belső autentikáció, user access mgmt, stb...
- NTP – időszinkronizáció – minden szerver ugyanazt az időt mutassa
- Monitoring – Proaktív hiba felderítés és elhárítás
- Automation – automatikus szerver létrehozása, automatikus patchelés, stb...

Felhő és ami mögötte van – Shared Core Services

- ITIL alapú Change management – hogyan tervezzünk és hajtsunk végre bármilyen változtatást, úgy hogy minél biztonságosabb legyen a végrehajtás, és minimális legyen annak az esélye annak, hogy valami rosszul sül el.
- ITIL alapú Problem management – felelős folyamat hogy visszatérő incidensekre végső megoldást kínáljon, illetve hogy megakadályozza incidensek újra előfordulását
- ITIL alapú Incident management - a cél, hogy olyan folyamatot alkossunk, hogy incidens során a leggyorsabban visszaállítsuk a teljes szolgáltatást, a lehető legkisebb hatással a többi ügyfélre illetve szolgáltatásra
- ITIL alapú Release management – folyamat a szoftver release-ekre: tervezés, tesztelés, ellenőrzött körülmények közötti kivitelezés.
- CMDB – egy olyan adatbázis, amiben tároljuk az összes, service-t leíró dolgot és ezek kapcsolatát

Felhő és ami mögöttes van – Shared Core Services

Host, Rendszer,
Alkalmazás Monitoring.



Konfiguráció kezelés,
Ütemezési feladatok

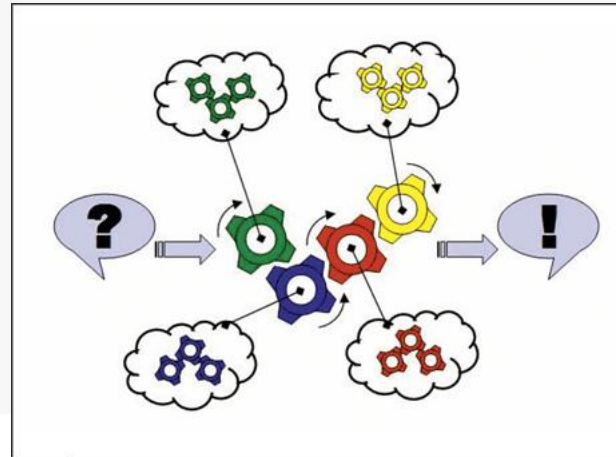
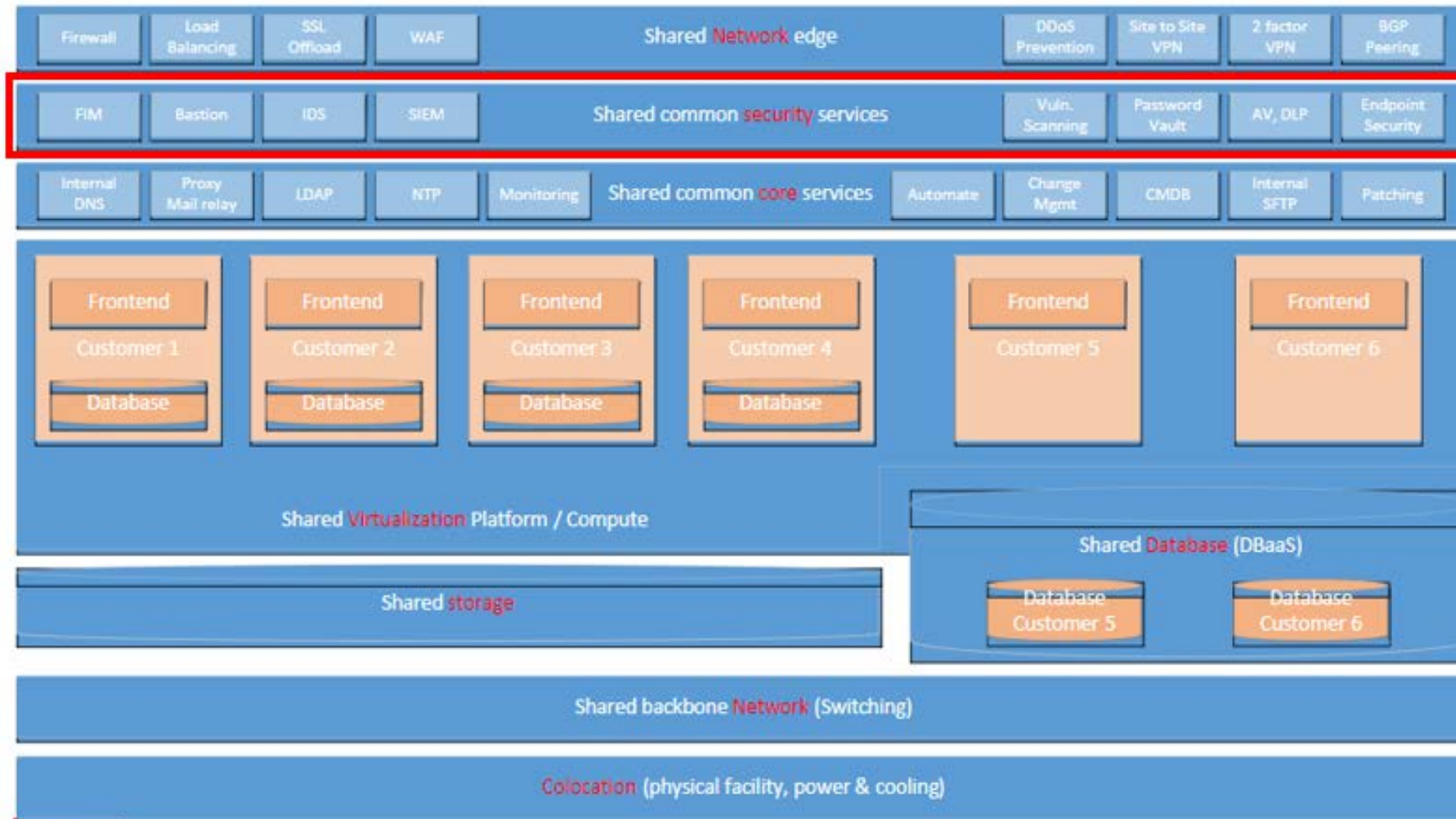


FIGURE 1 Service composition business modeling

Log és trend analízis



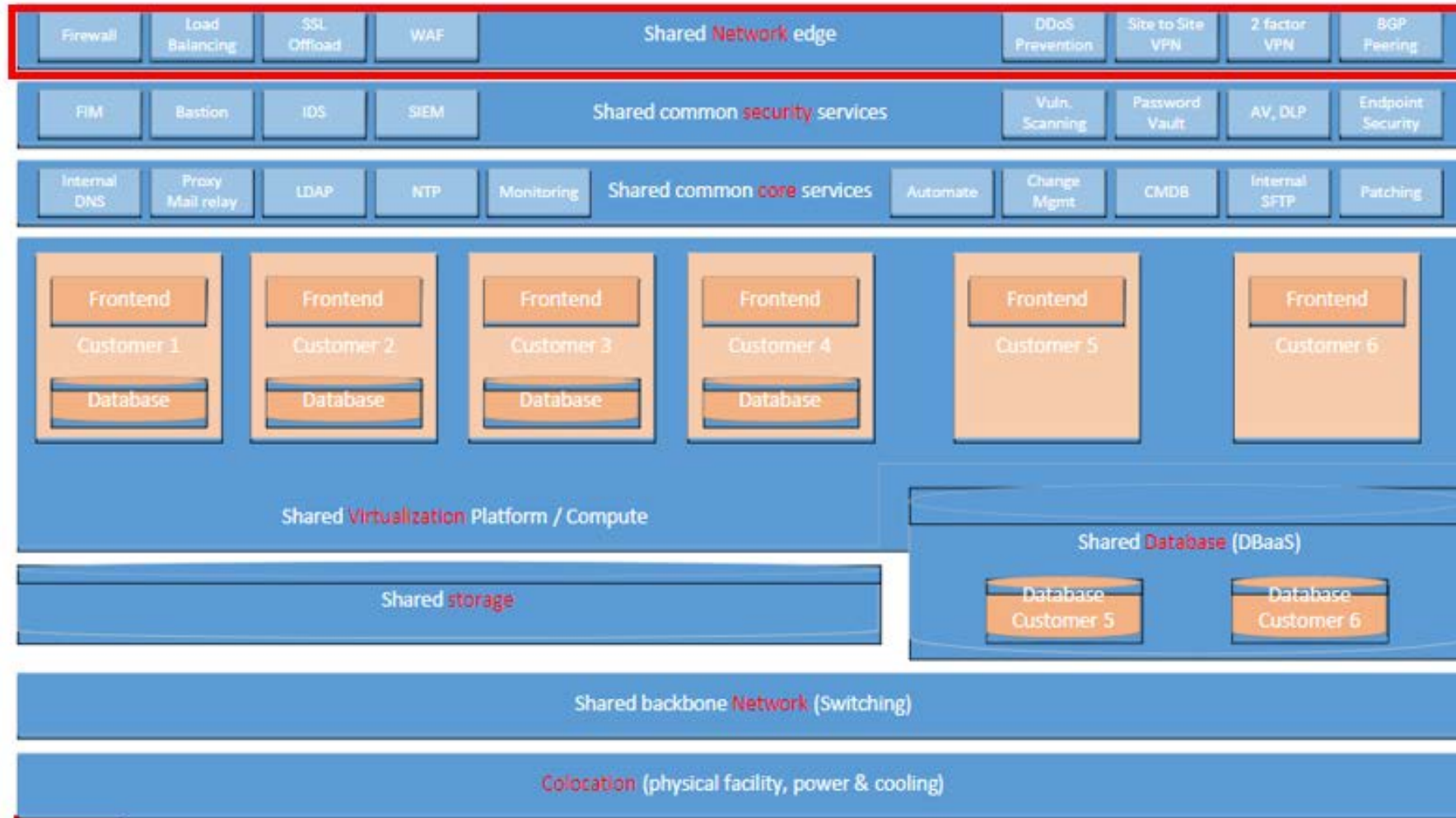
Felhő és ami mögötte van



Felhő és ami mögötte van – Security Services

- A felhők biztonsága az egyik legnagyobb kérdőjel az ügyfeleknél
- A felhő mégis biztonságosabb:
 - A felhőben mindenki egyforma – a cégvezetőnek, a dolgozóknak, az informatikusnak csak ahhoz van joga, ami a munkájához kell, és nem több. Saját rendszerénél éppen a túl sok jog ad támadási felületet
 - A fizikai hozzáférés rendkívül szigorú: biztonsági szolgálat, ujjlenyomat, akár retina szkennelvény vagy arcfelismerés
 - Beléptetés mindig bonyolultabb és biztonságosabb
 - Vírus- és behatolásvédelem nagyon magas szintű
 - Külső és belső sebezhetőség szkennelése, gyenge pontok feltérképezése
 - Szabványok és tanúsítványok kötelezik a szolgáltatókat arra, hogy a szervereket és a szolgáltatásokat folyamatosan karban tartsák (pl. Windows patch) illetve az adatokat megvédjék – biztonsági mentések.
Ezek betartását a tanúsítványt kiadó szervezetek folyamatosan ellenőrzik

Felhő és ami mögötte van



Felhő és ami mögötte van – Külső hálózat

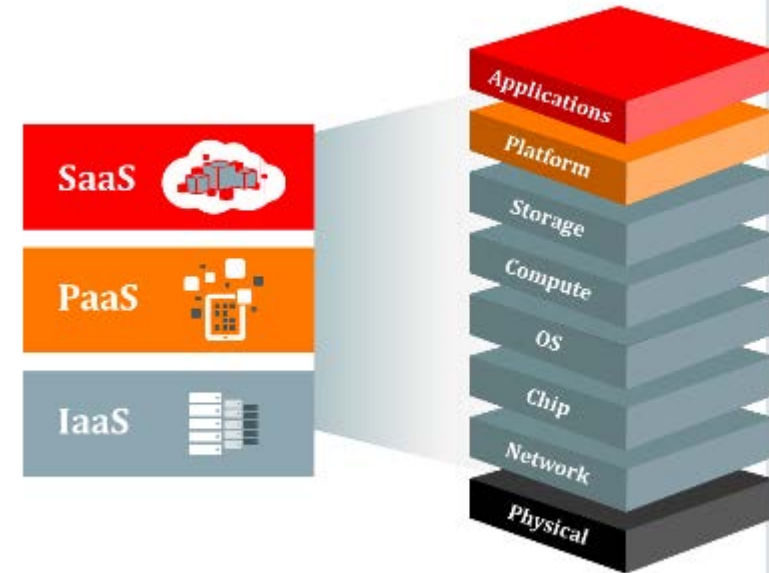
- Kívülről érkező kapcsolatok kezelése:
 - VPN
 - Load balancing
- Kívülről érkező támadásokra:
 - Hardware tűzfalak
 - WAF – Web Application Firewall – pl. URL átírása és malware elrejtése benne
 - DDoS támadások detektálása és visszverése

Software as a Service (SaaS)

- A SaaS megoldás lehetővé teszi a felhasználóknak, hogy regisztrálják magukat a felhőbe és használják a felhő nyújtotta alkalmazásokat, legyen az vállalat vagy magánember.
- A modern SaaS rendszerek lehetőséget biztosítanak arra is, hogy a felhasználók magukra szabhassák a környezetet, és biztosítják a könnyű csatlakozást bárhol, bármilyen eszközről, biztonságosan.

Software as a Service (SaaS)

- SaaS szolgáltatás esetén a szoftver license előfizetés alapon működik és központilag szolgáltatunk.
- SaaS szolgáltatások túlnyomó többsége multitenant, ami annyit jelent, hogy egy adott alkalmazás egy adott beállítással működik minden ügyfélnek.
- A skálázhatóság és terheléselosztás miatt, ez a standard alkalmazás több gépre is telepítve van, és párhuzamosan futnak.
- SaaS szolgáltatásokat az ügyfelek minden eszközről elérhetik anélkül, hogy bármilyen változtatást kellene végrehajtani az eszközön, illetve bérmit is kellene telepíteni.



Software as a Service (SaaS)

- SaaS alkalmazásokat testre lehet szabni az ügyfél igényi szerint, de azzal számolni kell, hogy ezek költségeit az ügyfélnek kell állnia.
- A SaaS alkalmazásokat a tradicionális alkalmazásokkal szemben gyakrabban update-elik, frissítésket adhatnak ki akár hetente is.
- A SaaS alkalmazások általában nem rendelkeznek hozzáféréssel az ügyfél egyéb, nem SaaS rendszereihez, ezért a SaaS alkalmazások rendelkeznek biztonságos protocollokkal, interface-ekkel, amik segítségével mégis össze lehet kötni a 2 rendszert

Software as a Service (SaaS)

A SaaS modellnek 2 fő fajtája létezik:

- Vertikális SaaS

Az a szoftver, ami egy ipari ágaztnak nyújt teljes szolgáltatást (pénzügy, ingatlan, mezőgazdaság)

- Horizontális SaaS

Termékek, amik ezen ágazatokon átívelő szoftver kategóriák (marketing, sales, HR), tehát nem ágazat specifikus.

Software as a Service (SaaS) – Előnyök

- Üzleti szempontok
 - Üzemeltetési költségek csökkentése
 - Fejlesztési költségek csökkentése,
 - Skálázhatóság – olyan mértékben kell fizetni, amilyen mértékben növekszik a cég - kockázatmentes
- Technológia
 - Továbbfejlesztett WEB alapú technológiák alkalmazása
 - Továbbfejlesztett SSL biztonsági protokollok (HTTPS)
 - Nagy sebességű internet vonalak, fejlett mobilinternet technológiák
 - Sztéleskörű integrációs protokollok és interface-ek

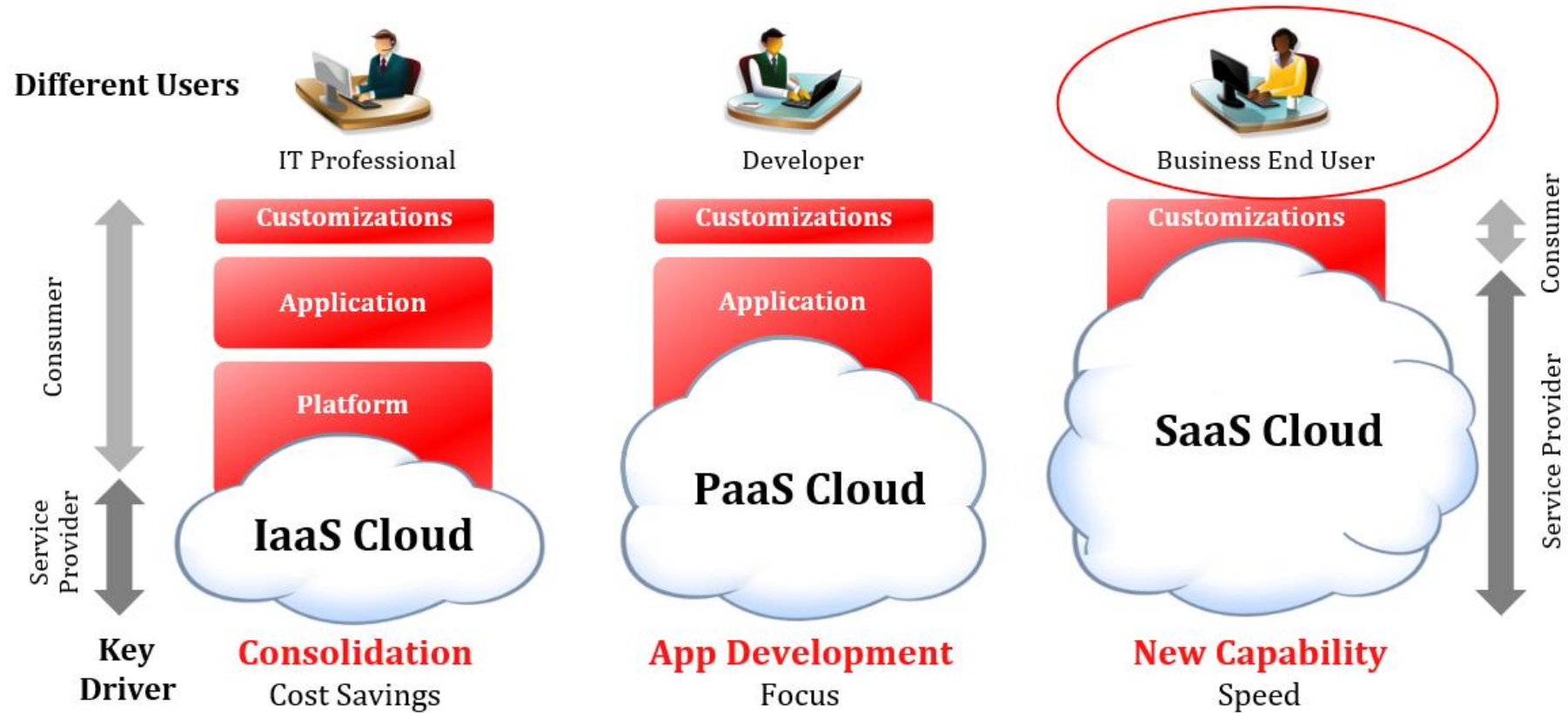
Software as a Service (SaaS) - Kihívások

- Adatbiztonság
- Hálózati késleltetés
- Multi tenancy korlátozza a testreszabási lehetőségeket
- Külső nagy adathalmaz integrálása
- Alkalmazás fejlesztésének leállítása, alkalmazás kivezetése
- Szolgáltató betartja az uptime-ot?
- Szolgáltató váltás

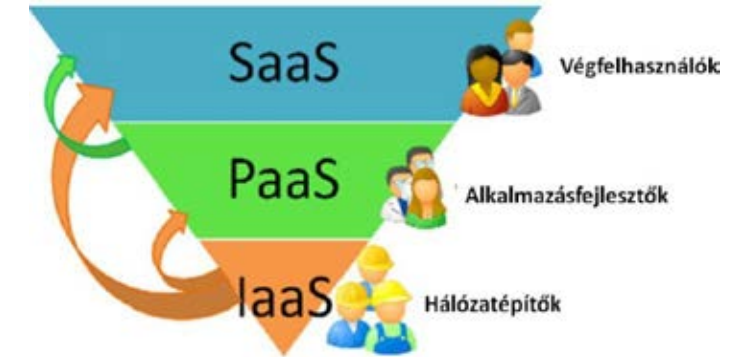
Tradicionális modell és SaaS modell

Tradicionális szoftver	Software as a Service
Dedikált telepítés	Multitenant telepítés
Skálázhatóság limitált	Skálázhatóság az egyik kulcs, dinamikus erőforráskezelés
Úgy tervezték, hogy mindenki saját magának telepít	Interneten keresztül, telepítés nélkül használható
A verzió váltások és upgrade-ek az ügyfelek által kivitelezettek	A szolgáltató dönti el mikor és mit upgrade-el
Az upgrade-nek költségei vannak, amit az ügyfél visel	Ingeyn upgrade, a költségeket a szolgáltató állja
Testreszabott integrációs megoldások más rendszerekkel	Interface alapú integrációs megoldások - standardizált

Felhő alapú szolgáltatások



Felhő alapú szolgáltatások



Saját adatközpont	IaaS	PaaS	SaaS
Alkalmazások	Alkalmazások	Alkalmazások	Alkalmazások
Alkalmazás adatok	Alkalmazás adatok	Alkalmazás adatok	Alkalmazás adatok
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
Operációs rendszer	Operációs rendszer	Operációs rendszer	Operációs rendszer
Virtualizáció	Virtualizáció	Virtualizáció	Virtualizáció
Szerverek	Szerverek	Szerverek	Szerverek
Tárhely	Tárhely	Tárhely	Tárhely
Hálózat	Hálózat	Hálózat	Hálózat

Pizza as a Service

Saját adatközpont	IaaS	PaaS	SaaS
Mosogatás	Mosogatás	Mosogatás	Mosogatás
Terítés, üdítők	Terítés, üdítők	Terítés, üdítők	Terítés, üdítők
Sütés	Sütés	Sütés	Sütés
Összekészítés	Összekészítés	Összekészítés	Összekészítés
Tészta kelesztés	Tészta kelesztés	Tészta kelesztés	Tészta kelesztés
Szósz elkészítése	Szósz elkészítése	Szósz elkészítése	Szósz elkészítése
Tészta gyúrása	Tészta gyúrása	Tészta gyúrása	Tészta gyúrása
Hozzávalók beszerzése	Hozzávalók beszerzése	Hozzávalók beszerzése	Hozzávalók beszerzése



Oracle mint szolgáltató

„Száz évvel ezelőtt a vállalatok megszüntették saját áramtermelő berendezéseiket, gépeiket, és csatlakoztak az elektromos hálózathoz... Napjainkban ugyanez a forradalom közeleg az informatika világában.”

(Nicholas Carr - Harvard Business Review – főszerkesztő)

Támogatott Szegmensek és számok – Oracle mint szolgáltató

- Constructions and Engineering Üzletág – 8000 milliárd dollár összértékű projectre több mint 100.000 cégnek nyújt segítséget
- Financial Üzletág – 1 milliárd számla, több mint 9000 pénzügyi szolgáltatónál, 1 milliárd kártyás tranzakció naponta
- Health Science Üzletág – TOP10 gyógyszergyártó cég software-es támogatása
- Hospitality Üzletág – több mint 35000 szálloda és 200.000 étterem
- Retail – 6000 online webshop és weboldal
- Utilities Üzletág – 550 millió ügyfél energetikai adatainak elemzése évi 700 millárd leolvasással, és kb 1.1 milliárd dollár spórolással

Oracle mint Infrastruktúra szolgáltató

- Szoftveres virtualizáció
- Költséghatékony és rugalmas számítási, tárhely és hálózati kapacitás
- Standard környezet, az ügyfeleknek nem kell újraírniuk a meglévő applikációkat, és már automatizált folyamataikat
- Infrastruktúra monitoring
- Hardware támogatás
- Erős biztonság
- Oracle Bare Metal Cloud Services.



Oracle mint Platform szolgáltató

Adatkezelés



Alkalmazás
fejlesztés



Üzleti intelligencia



Big
Data



Mobilitás



Content
& Social



Enterprise
Integráció



Rendszer
Felügyelet



Oracle mint szoftver szolgáltató

- A SaaS modell egyszerű és átlátható, azonnal bevezethető és a végfelhasználók által azonnal alkalmazható
- Mindent a szolgáltató ad, a felhasználó csupán némi konfigurálást hajt végre
- Internetes elérés, nem kell lokális telepítés
- Teljes körű felügyelet
- Licenzeket a szolgáltató kezeli
- Szoftver karbantartás
- Verziókövetés
- Mérés és monitoring



Modern Oracle Cloud



Oracle SaaS

Egyszerű és gyors kiépítés, azonnal
használatra kész



Legfejlettebb eszközök az
alkalmazások kezeléséhez



Egyszerű alkalmazás fejlesztés,
szofisztikált monitoring



Egyszerű, mégis minden igényt
kielégítő alkalmazáskezelés



Magasfokú biztonság



Forradalmian új integrációs
lehetőségek

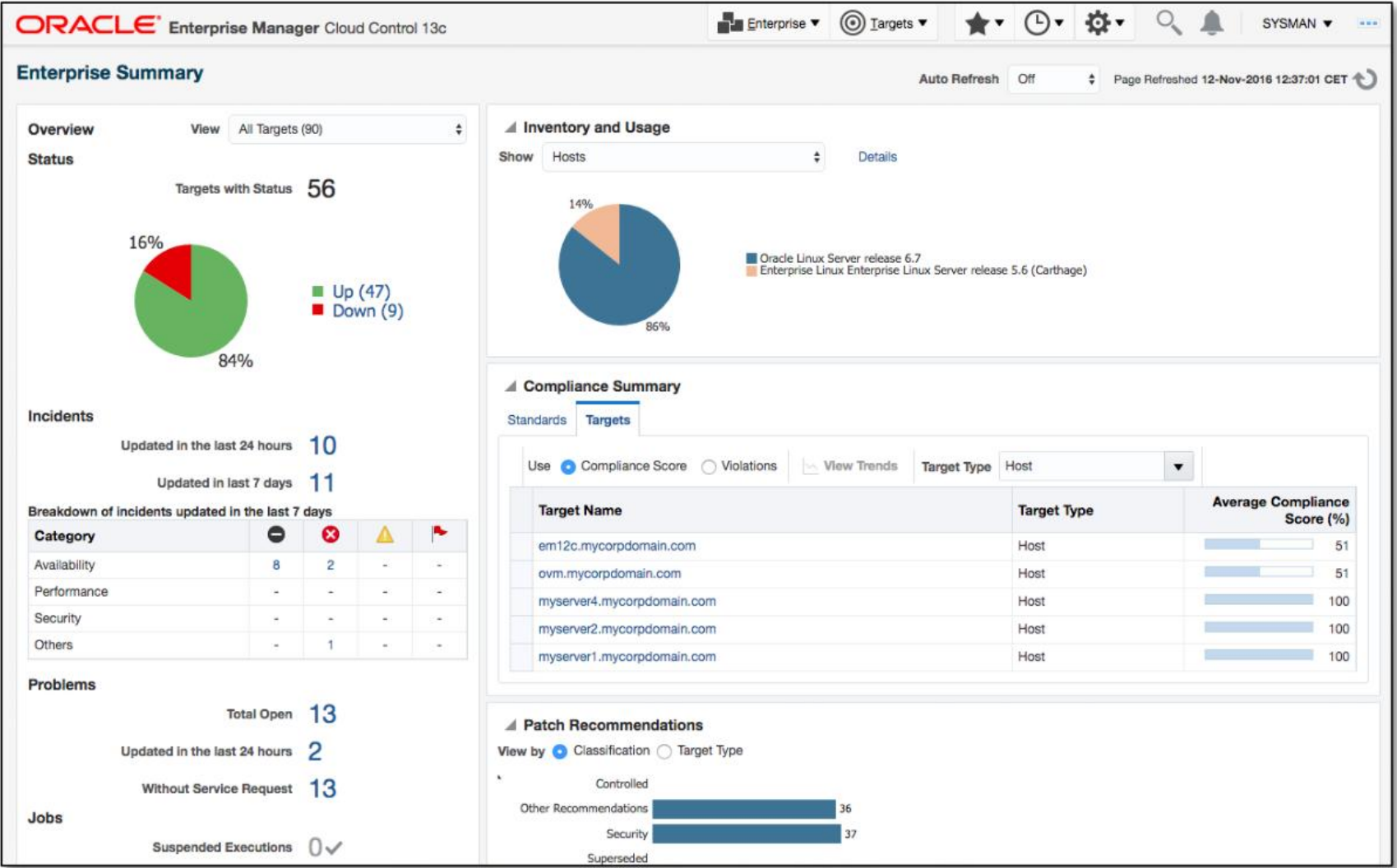


Monitoring - Enterprise Manager Cloud Control 13c

- Teljeskörű adminisztrációs, support és monitoring rendszer
- Különböző gyártók hardware-eit, és különböző operációs rendszereket képes kezelni.
- Szoftverek és operációs rendszerek patch szintjének karbantartása
- Alkalmazások és hardware teljesítmény monitoring
- Képes cloud es nem cloud alkalmazások együttes monitoringozására és karbantartására
- Hibákra és monitoring jelzésekre automatikus választ képes adni
- Statisztikák, reporting



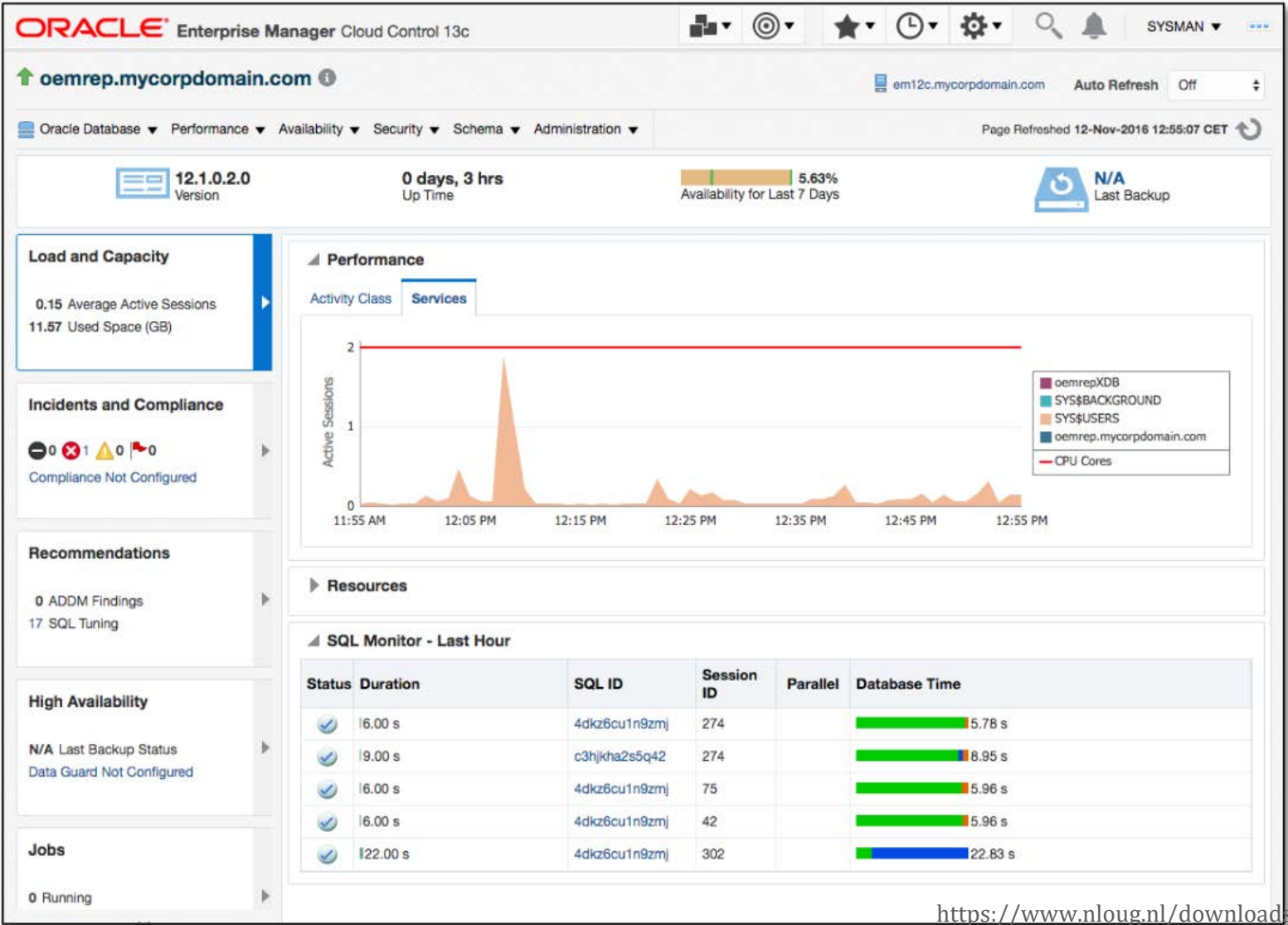
Monitoring - Enterprise Manager Cloud Control 13c



https://www.nloug.nl/downloads/ogh20161123_rob_zoetewei.pdf



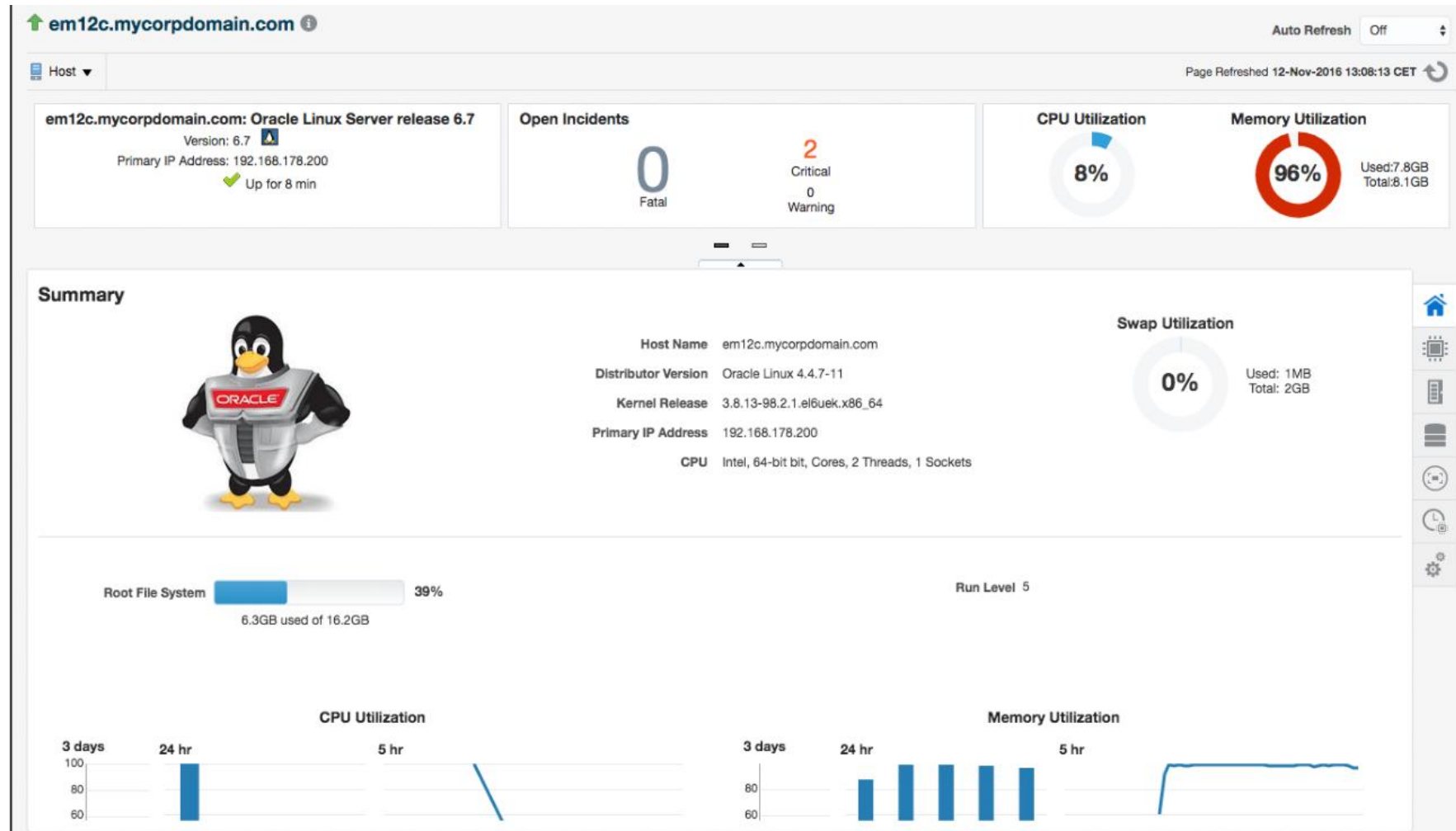
Monitoring - Enterprise Manager Cloud Control 13c



https://www.nloug.nl/downloads/ogh20161123_rob_zoeteweij.pdf

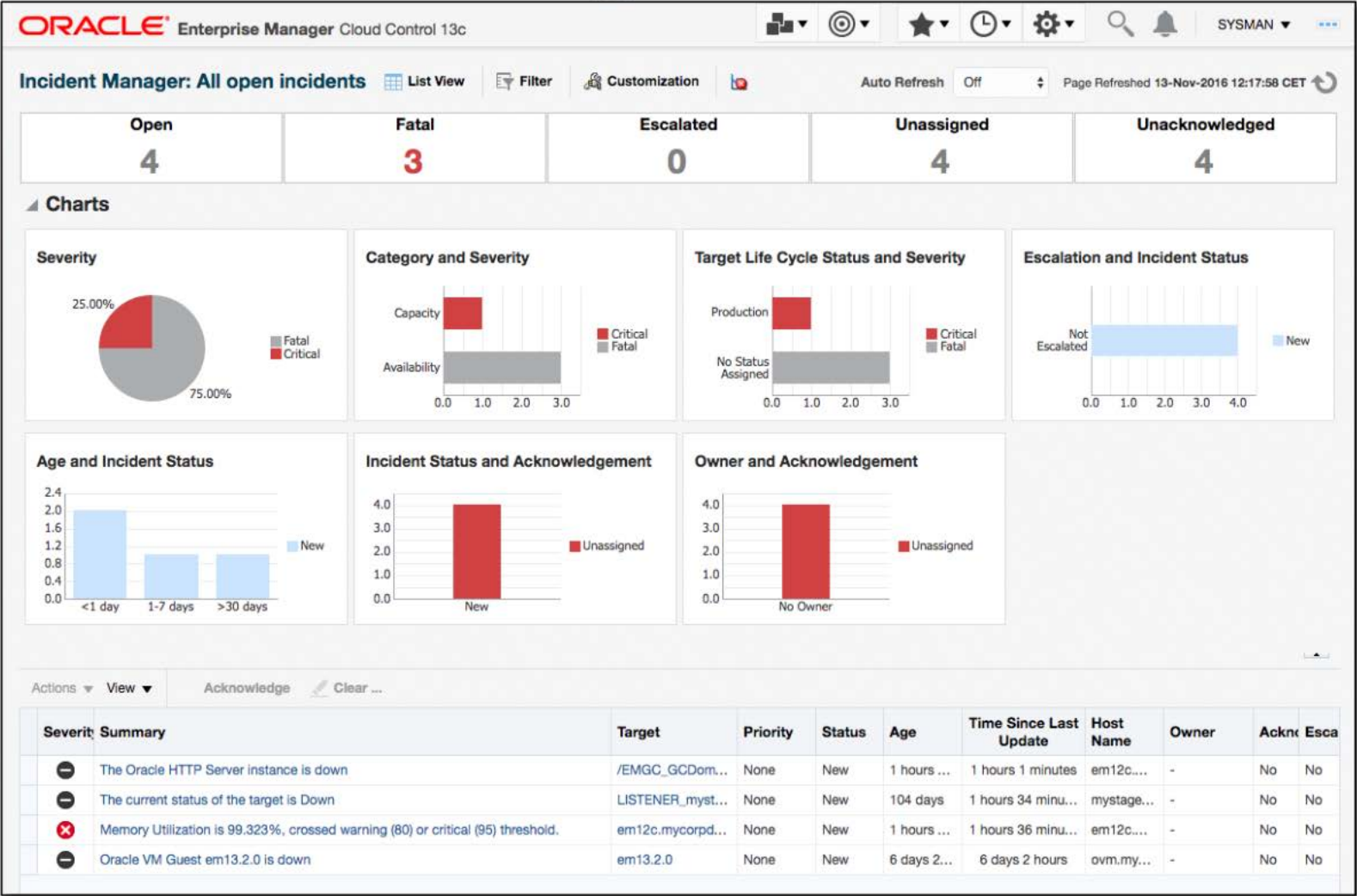


Monitoring - Enterprise Manager Cloud Control 13c



https://www.nloug.nl/downloads/ogh20161123_rob_zoeteweij.pdf

Monitoring - Enterprise Manager Cloud Control 13c



https://www.nloug.nl/downloads/ogh20161123_rob_zoetewei.pdf



ORACLE®

Security alert



Nemzeti Kibervédelmi Intézet
Kormányzati Eseménykezelő Központ



Ikt. sz.: 30700-0/2070-17/2018

TLP:WHITE
Szabadon terjeszthető!

Riasztás

Microsoft és Adobe termékeket érintő sérülékenységekről
(2018.10.10.)

https://www.nloug.nl/downloads/ogh20161123_rob_zoeteweij.pdf

Wannacry

- 150 ország
- 200.000-nél is több fertőzött gép
- 327 fizetés történt \$130,634.77 USD (kb 36.5 millió Ft) értékben.
- 4 nap után teljesen megállították a vírust