



Titkok

Belső támadások

Törvényi előírások

ORACLE®

**Oracle adatbázisok proaktív es reaktív
védelmi eszközei**

Mosolygó Ferenc, vezető technológiai tanácsadó



Proaktív és reaktív védelem

Proaktív eszközök

- Mozgó és nyugvó adatok védelme titkosítással
- Felhasználók szigorú azonosítása
- Hozzáférés szabályozás adattartalom alapján
- Privilegizált felhasználók (DBA-k, fejlesztők) szigorú szabályozása

Reaktív

- Felhasználói tevékenységek központosított naplózása



Adatok védelme titkosítással

Advanced Security Option

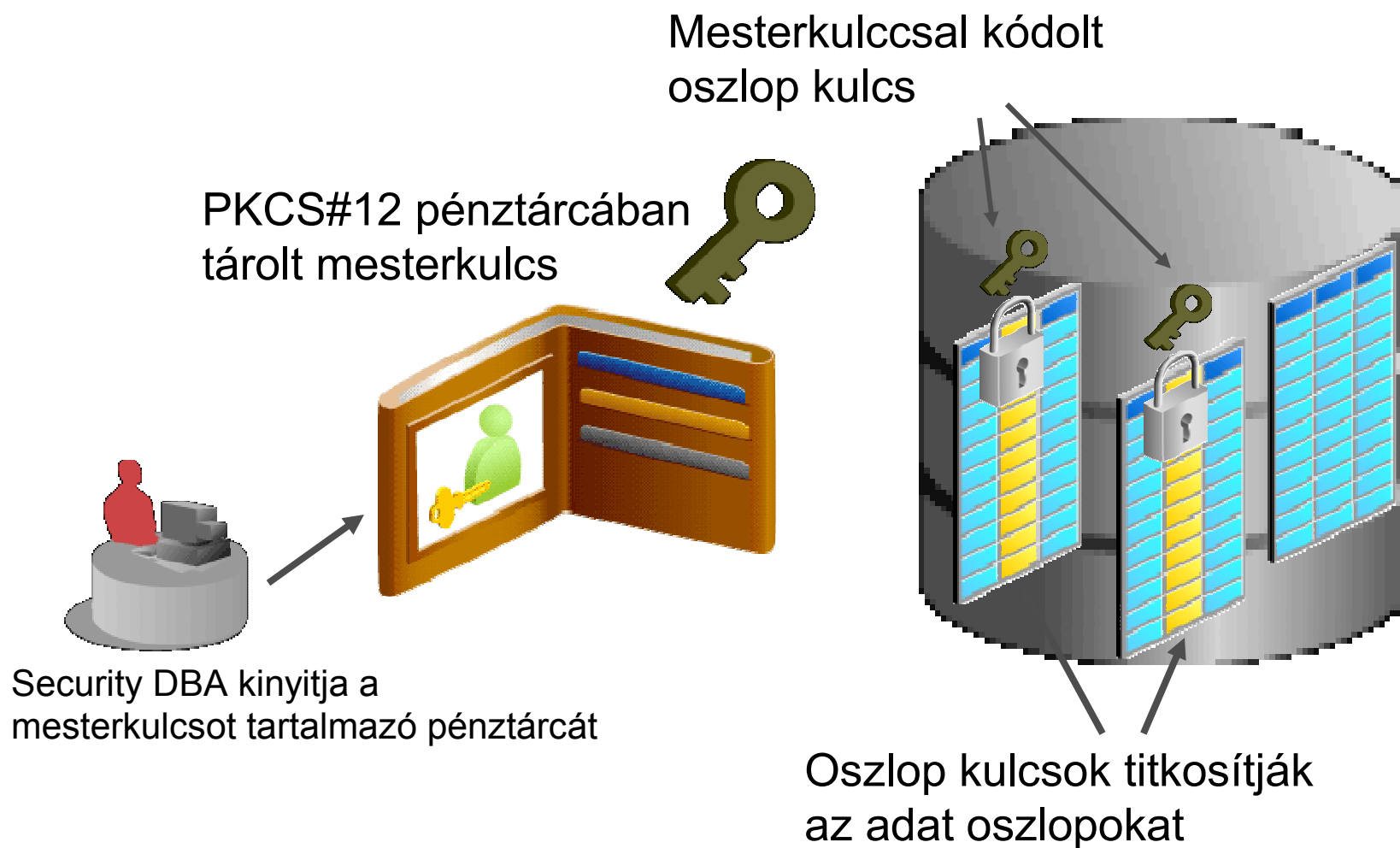
Mozgó adat

- Hálózaton keresztüli forgalom (LAN, Internet, Wireless)
- A kliens felé továbbított adatok lehallgatás elleni védelme
- SSL használata a kapcsolat védelmére

Nyugvó adat

- Adatbázisban tárolt
- Az adatbáziskezelő védi az adatokat a jogosulatlan hozzáféréstől
- Oszlop szintű megoldás

Mesterkulcs és oszlop kulcsok



Transzparens adat titkosítás

Oracle Advanced Security
Erős azonosítás



Alkalmazás

Oracle Advanced Security
Network Encryption

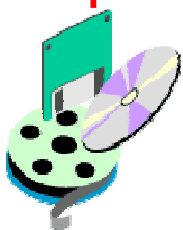


A diszkről olvasott
adat automatikusan
dekódolt



A lemezre
írt adat
automatikusan
kódolt

Oracle Advanced
Security
Transparent Data
Encryption



Titkosított mentés

Oracle Label Security



Jogosultság - Titkos:Alpha

Alkalmazás adattábla

| Projekt | Hely | Csoport | Érzékenységi Címke | |
|---------|---------|----------|----------------------------|----|
| AX703 | Szeged | Pénzügy | Nem besorolt | OK |
| B789C | Eger | Kutatás | Titkos: Alpha | OK |
| JFS845 | Miskolc | Jogász | Szigoruan titkos:Beszerzés | X |
| SF78SD | Győr | Munkaügy | Titkos:Turbine:Ázsia | X |



Oracle Database Vault



Miért Database Vault?

- Az előírásoknak való megfelelés: Sarbanes-Oxley, Graham-Leach Bliley, Basel II, Hpt 13/b, Tpt 101/a **erős belső szabályozást** és a **felelősségi körök szétválasztását** igényli.
- A belső támadások elleni védekezés kikényszeríti az üzemeltetési biztonsági szabályok betartását. - **Ki, mikor, hol** férhet hozzá az adatokhoz.
- Az adatbázis konszolidációs stratégia megelőző intézkedést kíván a **kiváltságos (DBA, fejlesztő)** felhasználókkal szemben.

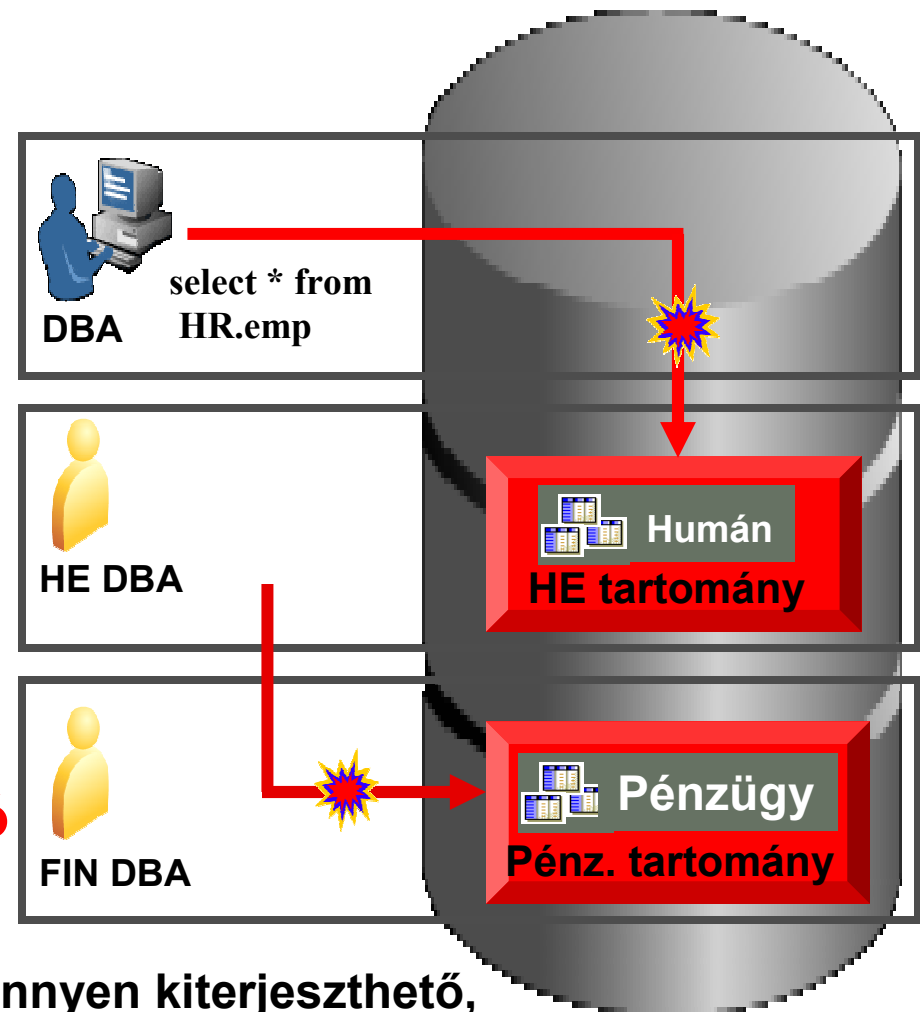
Oracle Database Vault Tartományok

- Az adatbázis adminisztrátor próbálja elérni a humán erőforrás adatokat

Védelem a belső támadóktól

- A humán erőforrás DBA próbálja elérni a pénzügyi adatokat

Kiküszöböli a konszolidáció biztonsági kockázatait

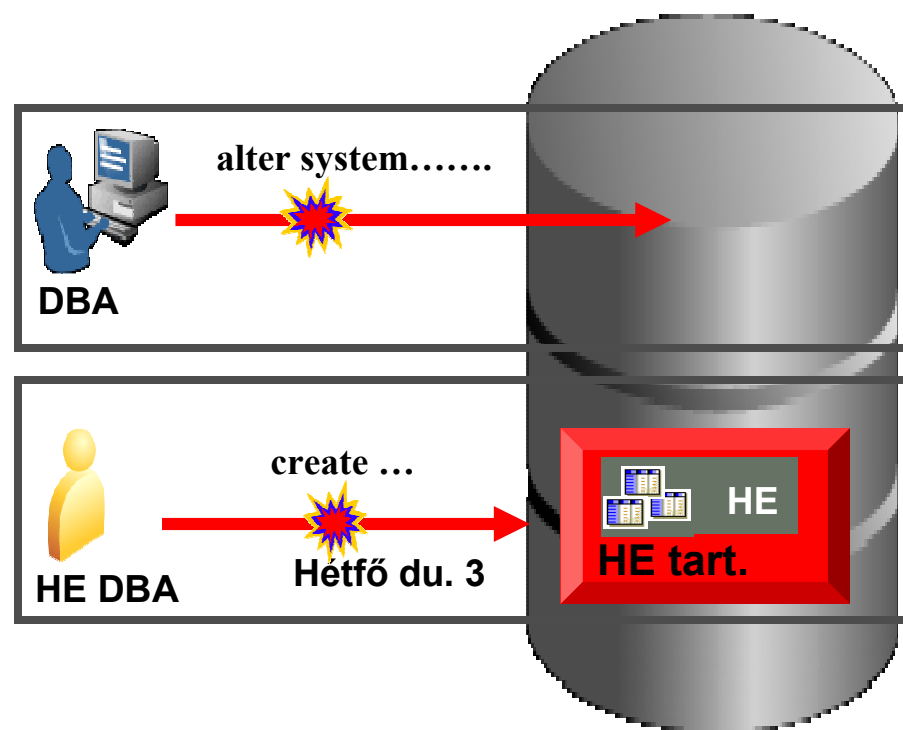


Meglévő alkalmazásokra könnyen kiterjeszthető,
minimális teljesítmény csökkenés mellett

Oracle Database Vault

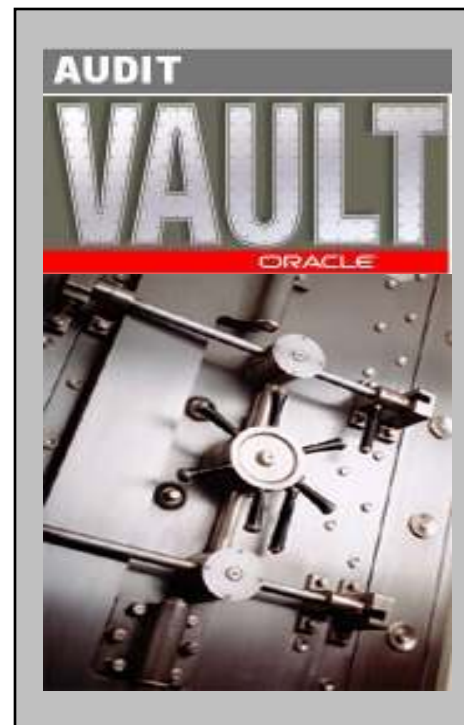
Többtényezős hozzáférés szabályozás

- A DBA távoli rendszer-módosítást kísérel meg “*alter system*”
Hálózati cím alapján működő szabály
- A HE DBA nem engedélyezett műveletet végez az éles rendszeren
Dátum és idő alapján működő szabály



A tényezők és az utasítás szabályok rugalmas és könnyen alkalmazható biztonsági szabályozást tesznek lehetővé

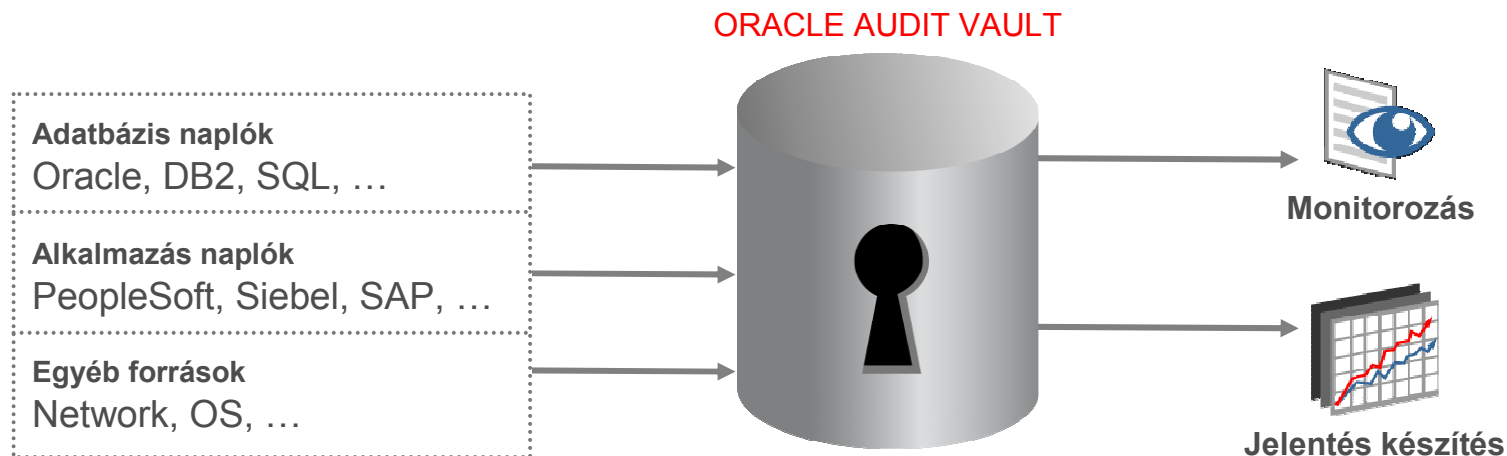
Oracle Audit Vault



Törvényi előírásoknak való megfelelés bizonyítása

- Biztonsági rendszer napló integritás védelme
- Oracle Audit Vault – specializált adattárház
 - **Összegyűjtött** audit adatok – Oracle és nem Oracle források
 - **Védett**, értékes audit adatok
 - **Adatok** a kiváltságos felhasználók tevékenységeiről
 - **Jelentés** a szabályoknak való megfelelésről

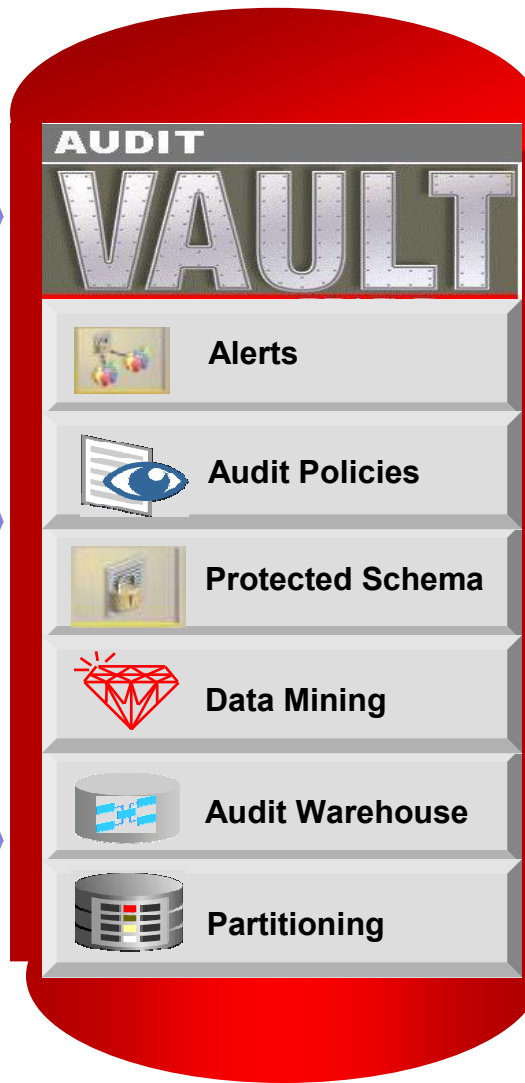
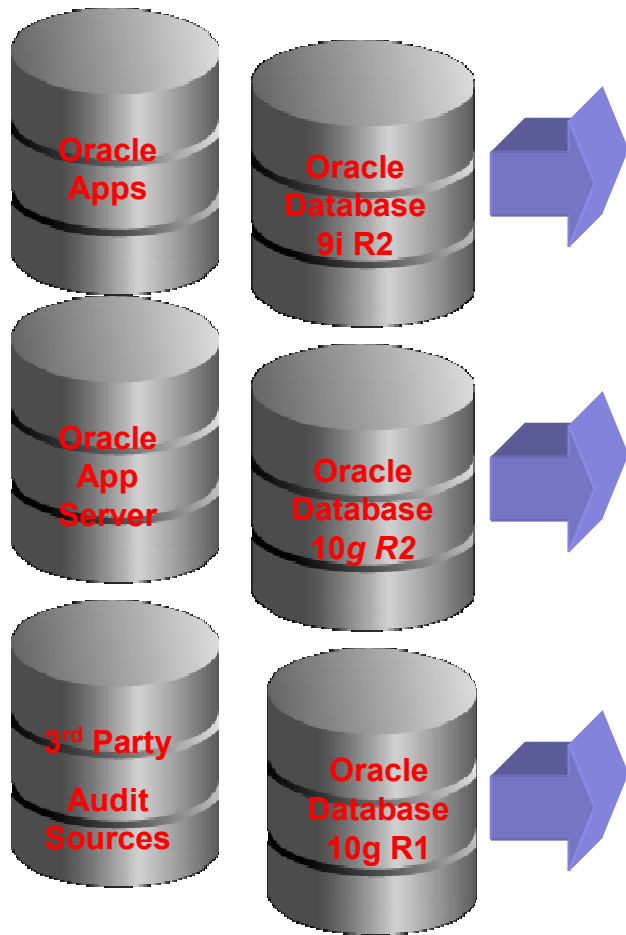
Hamarosan!



Oracle Audit Vault*

Policies, Collection, Alerts, and Reports

Enterprise Audit Sources



Audit & Compliance Dashboard



Audit & Compliance Reports



Custom Reports



Audit & Compliance Alerts



ORACLE®