Pákozdi, Lóránd, IBM Magyarországi Kft.
2010. június 14.

Hatékony adatbázis-kezelés

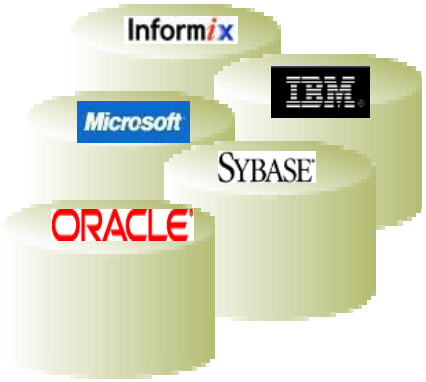
Védelem, valós idejű biztonság és megfelelőség, audit.

Napirend

- Problémák az adatbázisok ellenőrzése kapcsán
- Kritikus adatok védelme a teljes életciklusuk alatt
- Egy jó megoldás – GUARDIUM
  - .... mint cég
  - valósidejű adatbázis monitorozás és biztonság
  - monitorozási képességek
  - alkalmazások felhasználóinak azonosítása
  - architektúra, skálázhatóság, integráció
- Forrester Wave™: Adatbázis-ellenőrzés és valós idejű védelem (2011. Q2)
- Referenciák

Problémák az adatbázisok ellenőrzése kapcsán

- ☒ Átláthatóság és aprólékosság
  - A kiváltságos felhasználók ellenőrzése nehéz
  - Egyes alkalmazások felhasználóinak nyomkövetése bonyolult
  - Nehézkes az egyes nem engedélyezett változások felismerése
  - Az auditálás nem megfelelő
- ☒ Nem elég hatékony és költséges
  - Kihatással van az adatbázis teljesítményére
  - Nagy log állományok kevés többletinformációt adnak
  - Különböző módszerek szükségesek különböző alkalmazásokhoz
- ☒ Nem elégséges szerepkör szétválasztás
  - Adatbázis admin kezeli a monitorozó rendszert
  - A kiváltságos felhasználók átugorhatnak rendszereket
  - Audit folyamat nem biztonságos



Kritikus adatok védelme a teljes életciklusuk alatt

Különböző adatbázisok, alkalmazások és kliensek felderítése

Az érzékeny, kritikus adatok felderítése és osztályozza

Sebezhetőség felmérés

Konfiguráció felmérés

Viselkedés felmérés

Alaprendszer meghatározás

Konfiguráció lezárás és változás követés

Titkosítás

Központosított irányítás

Megfelelőségi jelentések

Aláírások kezelése

Automatizált eszkalálás

Biztonságos audit repository

Célzott adatbányászat (forensic – csalások megelőzése, felderítése és kivizsgálása)

Hosszú távú megőrzés

100% átláthatóság

Szabály-alapú akciók

Anomália érzékelés

Valós idejű megelőzés

Hangolható hozzáférés ellenőrzés

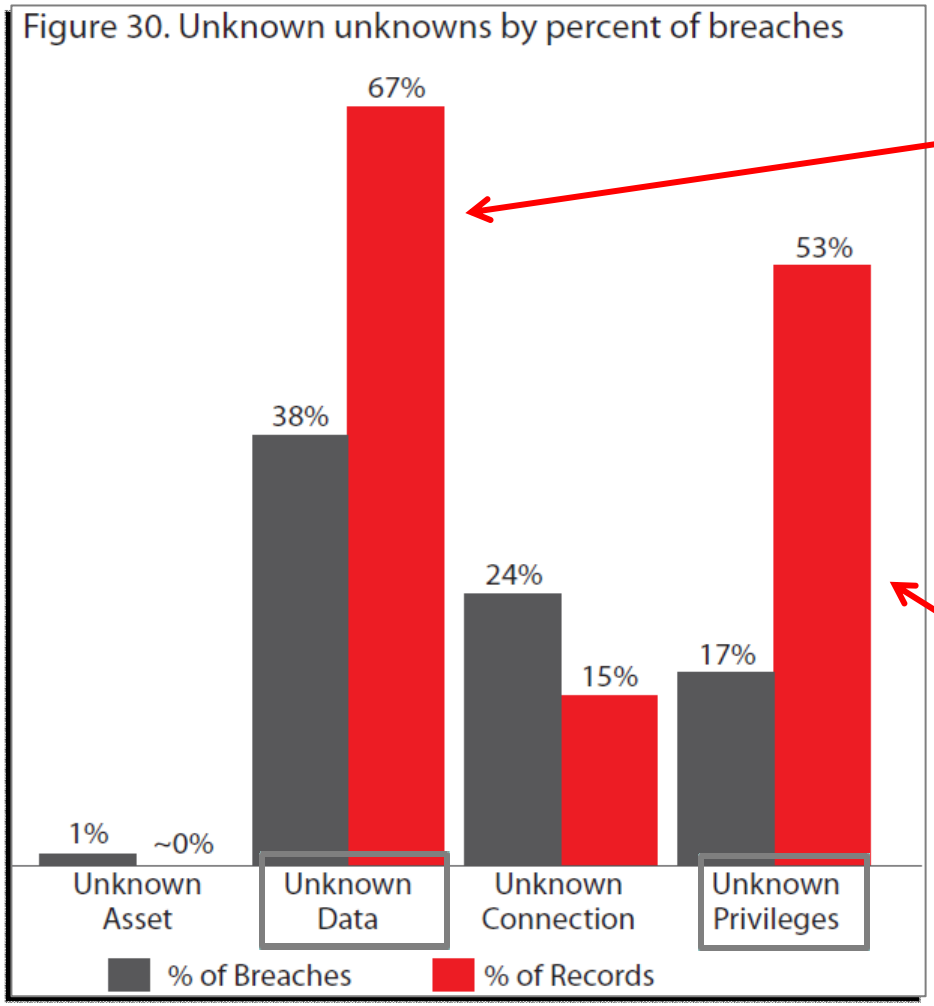
SIEM integráció

Adatvesztés, adatszivárgás okai
2009 Data Breach Report (Verizon RISK Team)

Asset	Asset Group	% of Breaches	% of Records
POS system	Online Data	32%	6%
Database server	Online Data	30%	75%
Application server	Online Data	12%	19%
Web server	Online Data	10%	0.004%
File server	Online Data	8%	0.1%
Public kiosk system	Online Data	2%	0.4%
Authentication / Directory server	Online Data	2%	0.1%
Backup tapes	Offline Data	1%	0.04%
Documents	Offline Data	1%	0.000%
Workstation	End-User System	8%	0.01%
Laptop	End-User System	4%	0.000%
PIN Entry Device	End-User System	2%	0.004%

http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

Adatvesztés, adatszivárgás okai: "Unknown Unknowns"



Ismeretlen adat
„Nem tudjuk, hogy a bizalmas adatokat hol tároljuk.”

Ismeretlen jogosultság
„Nem tudjuk, hogy az adott jogosultságok milyen módon lettek beállítva.”

http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

Adatvesztés, adatszivárgás felderítése – Hogyan?

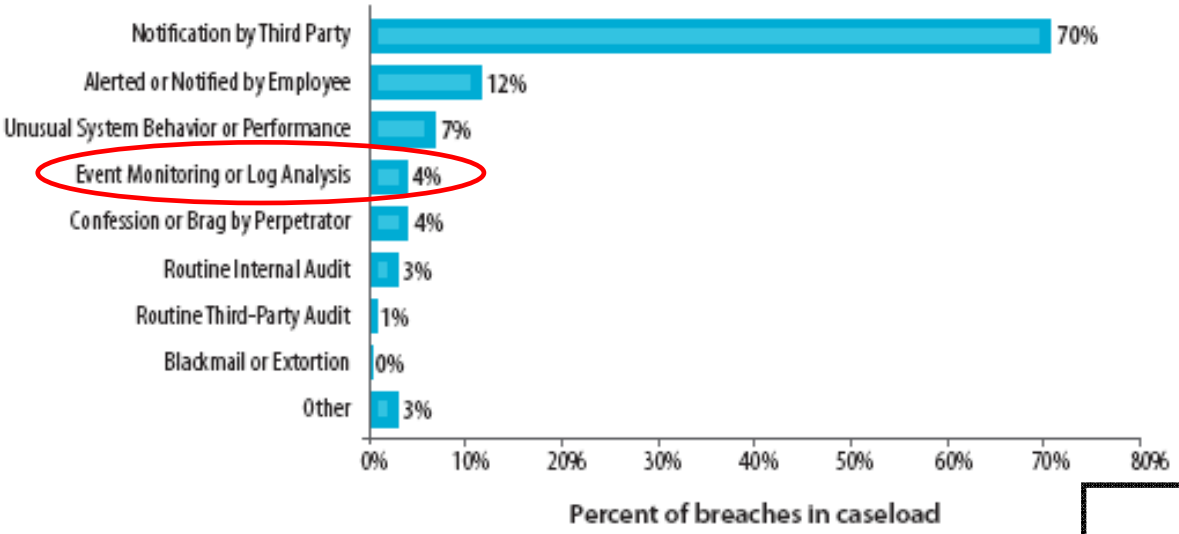
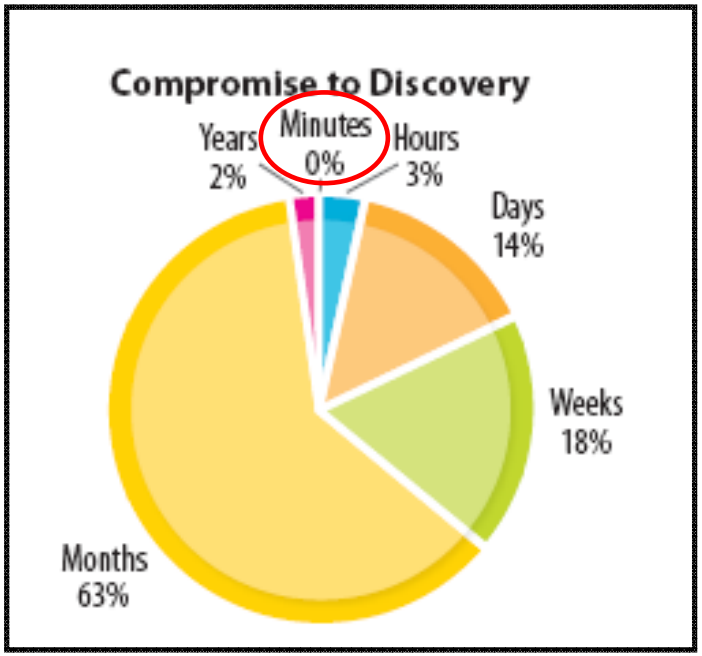


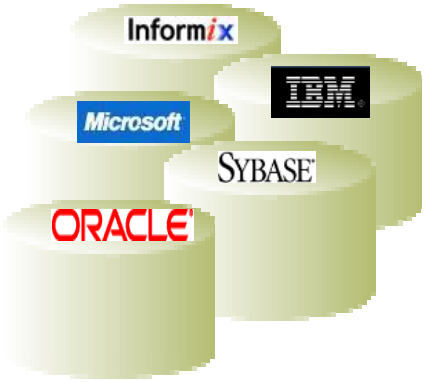
Figure 22. Data Breach Discovery Methods



Egy jó megoldás

- Magas szintű adatbiztonságot nyújt
  - Csökkenti a külső és belső sebezhetőséget
  - Valósidejű és proaktív kontrol az adatbázisokon
- Biztosítja az adatok megfelelő kezelését
  - Megvédi a kényes adatokat az illetéktelen módosításoktól
  - Bemutatja a megfelelőséget az auditorok felé
- Csökkenti a megfelelőséghez kapcsolódó költségeket
  - Egyszerű, automatikus, központi felügyelet
  - Kisebb rendszer erőforrás igény

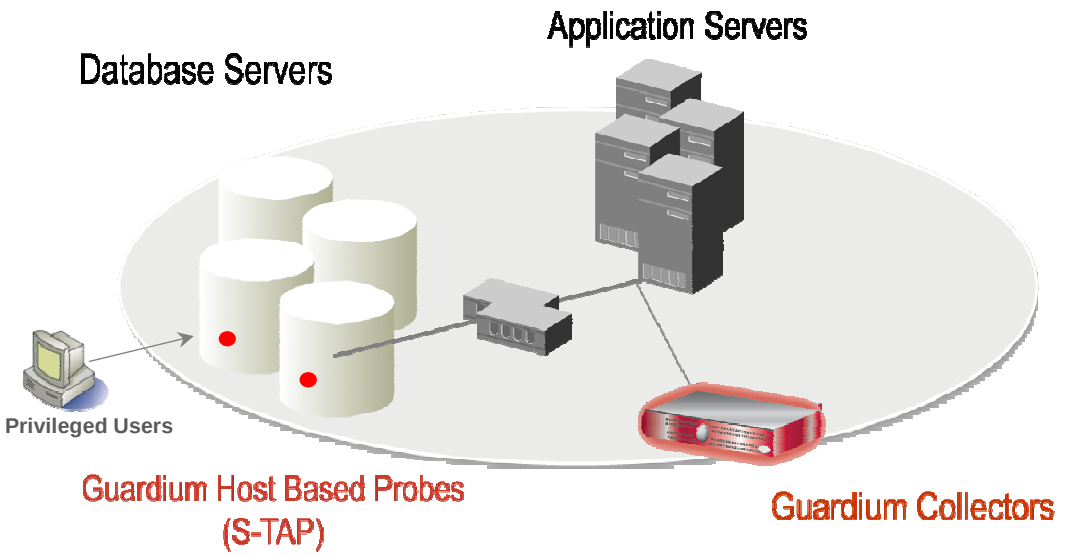
Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

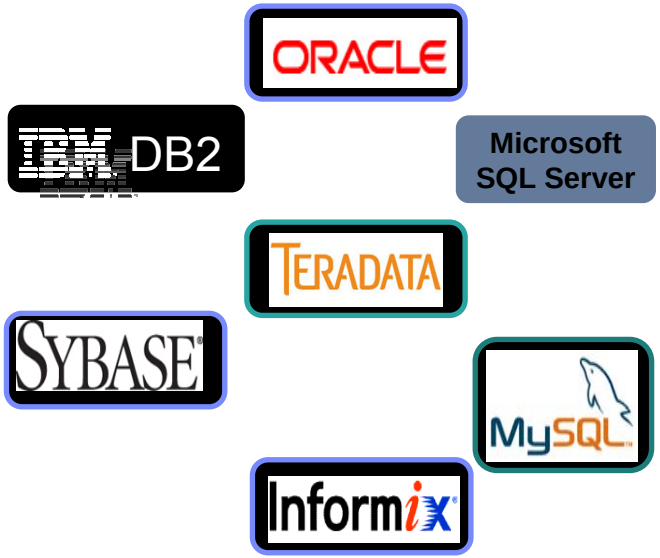


Guardium, mint cég

- 2002 óta egyértelmű iparági vezető az adatbázisok monitorozása területén
- Kizárólagos figyelem a adatbázisok auditálhatóságán és biztonságos kezelésén
- 400+ ügyfél a világban különböző iparágakban
- 2009 decembere óra része az IBM Integrated Data Management portfoliónak

Guardium - Valósidejű adatbázis monitorozás és biztonság



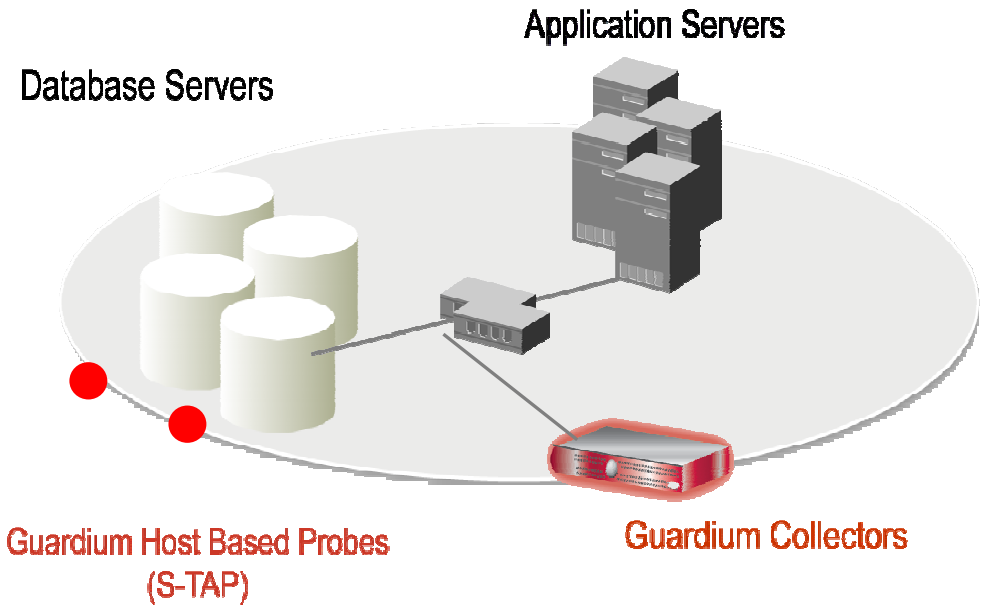


- Teljekörű hozzáférés-monitorozás
- Használatához nem szükséges adatbázis vagy alkalmazás módosítás
- Minimális adatbázis-teljesítmény terhelés
- Egyértelműen elkülöníthető szerepkörök (biztonságos audit állományok)

- Ki, mit, mikor és hogyan - monitorozás
- Valós idejű, szabályrendszeren alapuló monitorozás
- A céleszköz 3-6 hónapnyi adatot tud tárolni a saját tárhelyén
- Automatizált megfelelőség jelentések, aláírások (SOX, PCI, NIST, stb.)

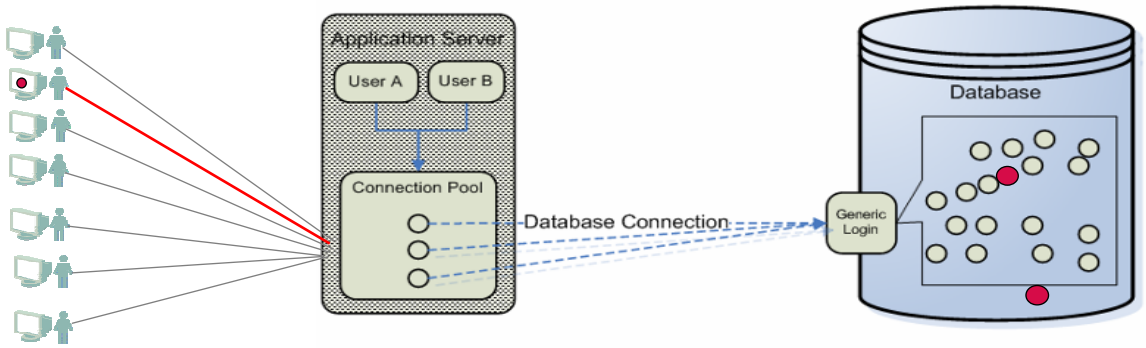
Guardium monitorozási képességek

- SQL hibák, Login események
- DDL parancsok (Create/Drop/Alter Tables)
- SELECT futtatás
- DML parancsok (Insert, Update, Delete)
- DCL parancsok (Grant, Revoke)
- Procedúra alapú leíró nyelvek
- Adatbázisból hívott XML

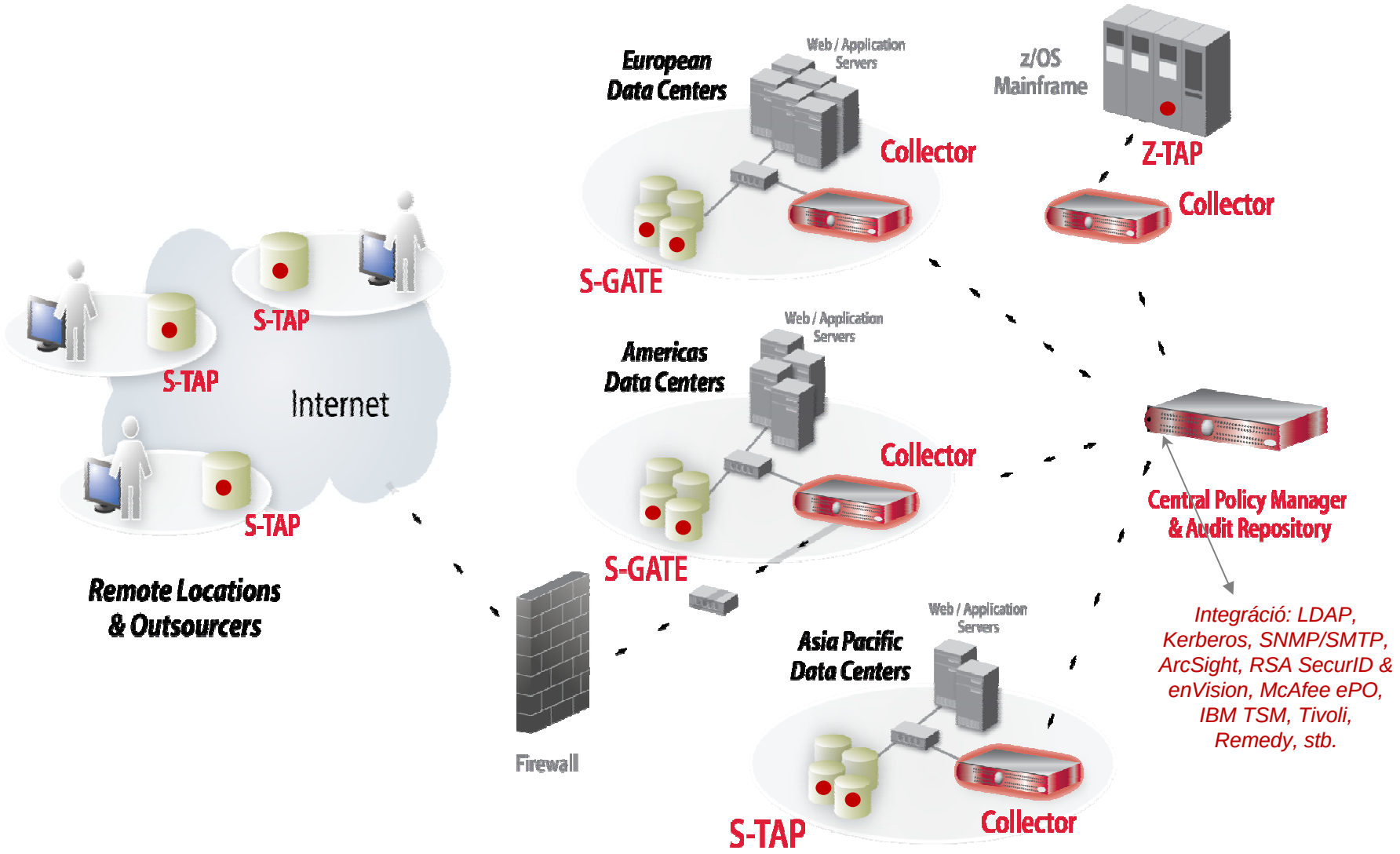


Guardium felhasználása alkalmazások felhasználóinak azonosítására

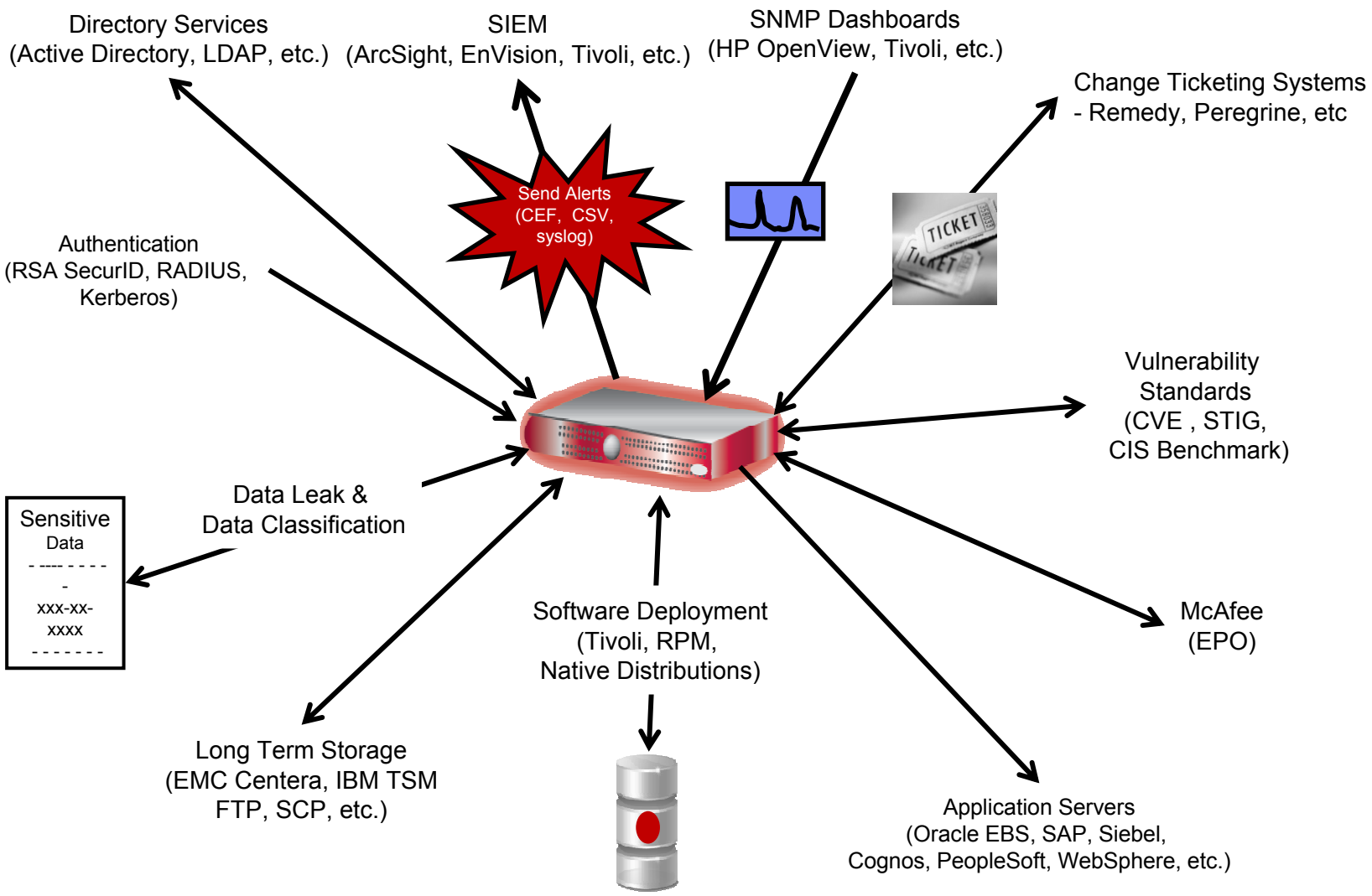
- Felhasználók azonosítása
  - Felfedi a lehetséges csalásokat
  - Pontosan ellenőrzi a felhasználói hozzáféréseket az érzékeny táblákhoz
- Támogatott nagyvállalati alkalmazások
  - SAP, Siebel, Oracle E-Business Suite, PeopleSoft, Business Objects Web Intelligence, JD Edwards, (és belső fejlesztésű egyedi alkalmazások integrációja is lehetséges)
- Felhasználói azonosítók (ID) rögzítése
  - Egyedi azonosítót összegyűjtése az adott adatbázisokból (táblák, trigger, stb. által)
  - Egyedi hívásokat ellenőrzése és a paraméter-információk összegyűjtése
  - S-TAP szonda által az alkalmazás, vagy proxy szerver által a felhasználói azonosító megszerzése



Skálázható, heterogén architektúra



Integráció a meglévő infrastruktúrával a költséghatékonyság érdekében

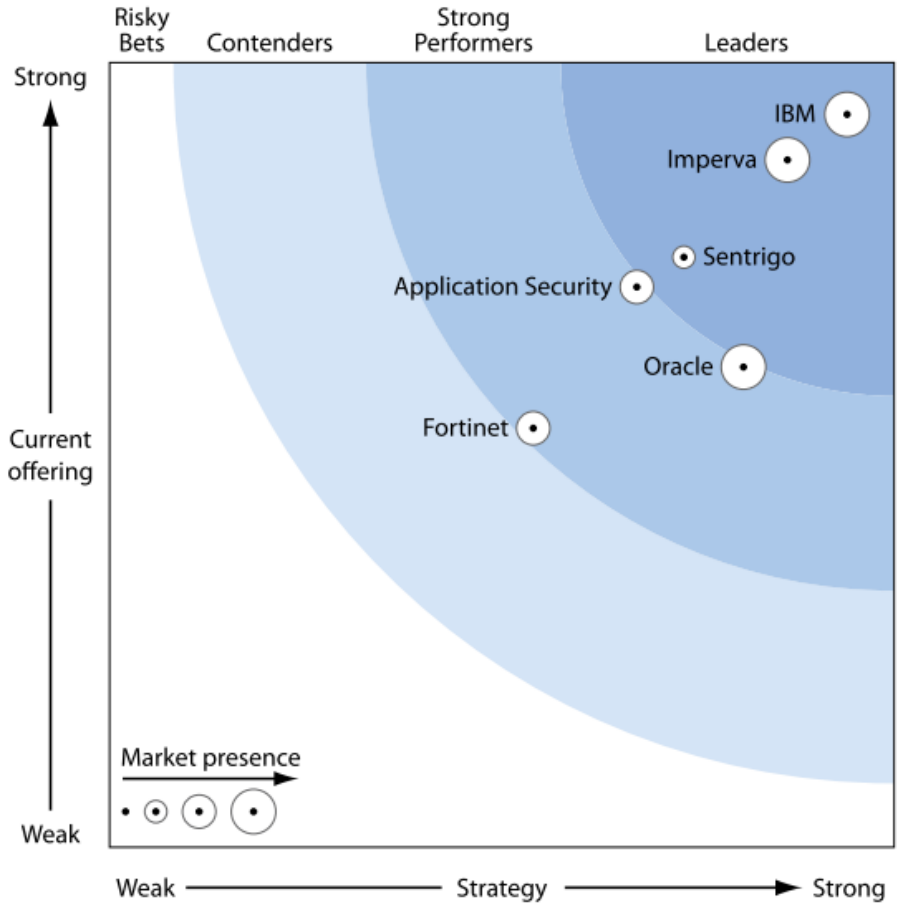


Az üzleti élet java használja....

Forrester: a legnagyobb összpontszám (aktuális ajánlatok alapján)

FORRESTER

“Demonstrating its Dominance in this Space”



- „IBM InfoSphere Guardium továbbra is vezetőnek bizonyul a rendkívül nagy, heterogén környezetekben, kiváló teljesítményt és méretezhetőséget biztosít, leegyszerűsíti a felügyeletet, és az adatbázisok valós idejű védelmét nyújtja.” Az IBM erős termék- és vállalati stratégiával rendelkezik, biztosítva a növekvő piaci jelenlétet.
- „Arra számítunk, hogy Guardium megőrzi vezető szerepét a nagy, heterogén környezetek támogatásában, kimagasló teljesítményt és méretezhetőséget biztosít, egyszerűsíti az adatbázis adminisztrációt és valós idejű adatbázis védelmet nyújt.”
- „... erős fejlesztési ütemterv több innovációt és elérhető funkciót tartalmaz a többi szállítóhoz képest.”
- Az első helyezett architektúra az következő funkciókra kapott pontszámok alapján: teljesítmény és skálázhatóság, felhasználhatóság, auditálási szintek, ellenőrzés és jelentés készítés (valós idejű riasztás), és alkalmazások támogatása.
- Guardium nyújtja a „kimagaslóan jó megfelelőségi jelentéseket és szerepkörök szétválasztását” kész termékként (out-of-the-box) több neves alkalmazás számára, mint például a SAP, Siebel, JD Edwards, az Oracle EBS, PeopleSoft.

Source: “The Forrester Wave™: Database Auditing And Real-Time Protection, Q2 2011” (May 2011)

Összegzés

- Egyszerű, következetes, különböző adatbázisokat lefedő megoldás
- Kényes adatok védelmének magas szintű biztosítása (magasabb szintű, mint a SIEM, log-elemző, stb. megoldások esetén)
- 100%-os átláthatóság heterogén adatbázis-infrastruktúra esetén is
- Előre definiált és automatizált folyamatok
- Szabadon skálázható megoldás

KÖSZÖNÖM

A FIGYELMET!

lpakozdi@hu.ibm.com