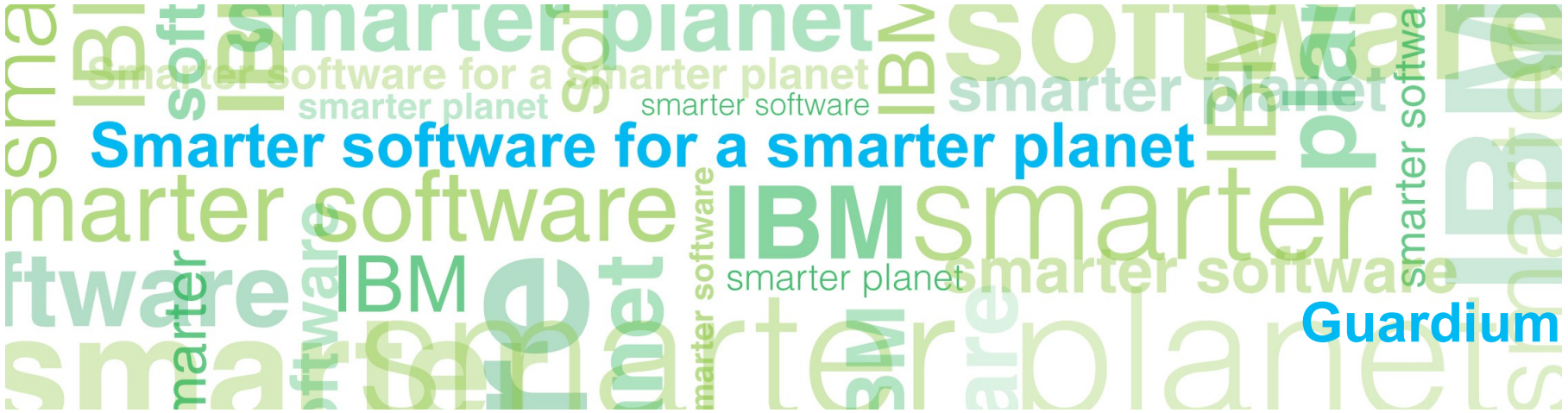
Pákozdi, Lóránd, IBM Magyarországi Kft.

Hatékony valós idejű adatbázis védelem és audit

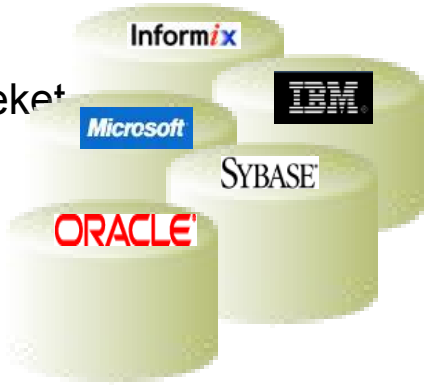


Napirend

- 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
  - sebezhetőség vizsgálat
  - architektúra, skálázhatóság, integráció
- Forrester Wave™: Adatbázis-ellenőrzés és valós idejű védelem (2011. Q2)
- Referenciák

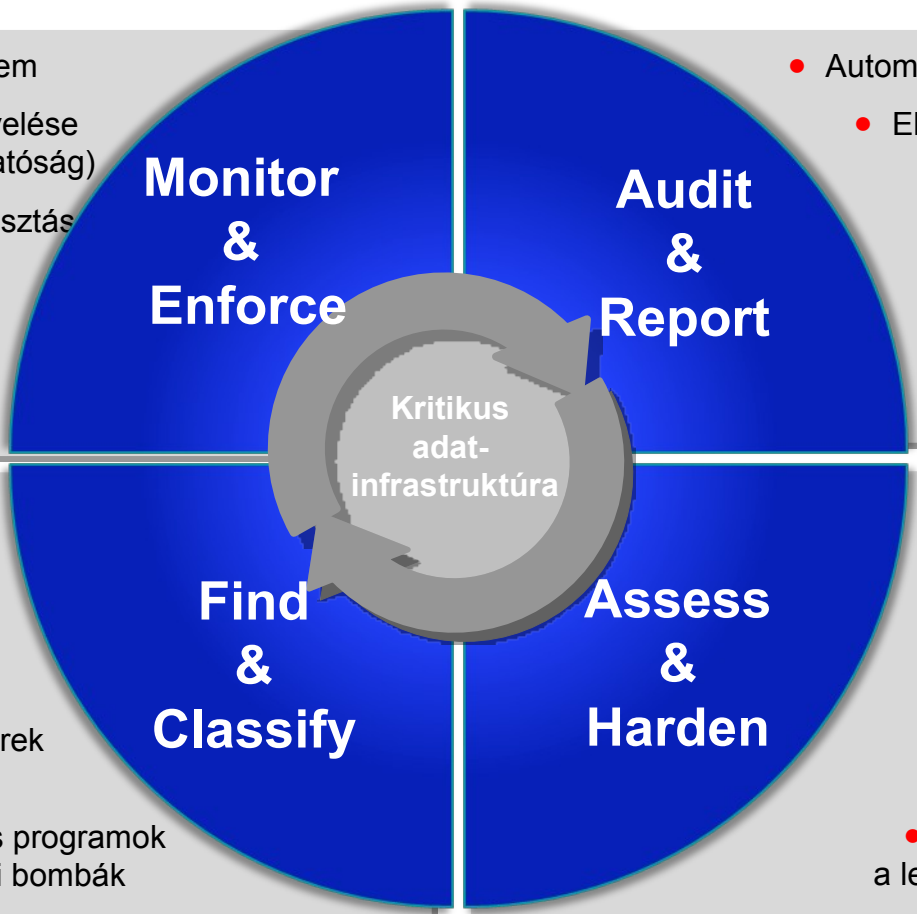
Problémák az adatbázisok ellenőrzése kapcsán

- ☒ 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

Valósidejű adatbázis biztonság és monitorozás



- ‘Cyber’ támadás elleni védelem
- Kiváltságos felhasználók figyelése és ellenőrzése (100% átláthatóság)
- Valós idejű megelőzés és riasztás
- Hangolható hozzáférés és alkalmazás szintű ellenőrzés
- Szabály-alapú akciók
- SIEM integráció

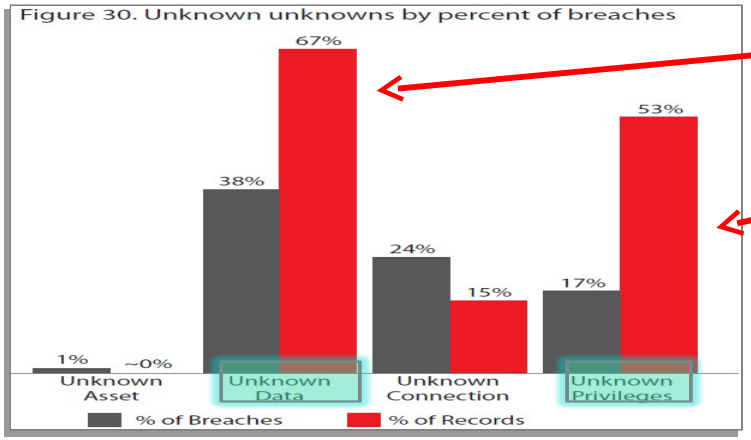
- Automatikus, központosított irányítás
- Előre meghatározott szabályok, megfelelőségi jelentések
- Automatizált eszkalálás
- Különböző adatbázisokon, változtatás nélküli, minimális teljesítményigényű működés
- Hosszú távú megőrzés

- Különböző adatbázisok, alkalmazások és kliensek felfedezése
- Az érzékeny, kritikus adatok felderítése és osztályozása
- A biztonsági szabályrendszerek folyamatos frissítése
- Rosszindulatú számítógépes programok (malware) és beépülő logikai bombák azonosítása

- Sebezhetőség, konfiguráció és viselkedés felmérés
- Konfiguráció lezárás és változás követés
- Titkosítás
- Előre meghatározott tesztek a leghasznosabb tapasztalatokat alapján (STIG, CIS, CVE)

Adatvesztés, adatszivárgás felderítése – mit, hogyan? (2009)

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



Ismeretlen adat

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

Ismeretlen jogosultság

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

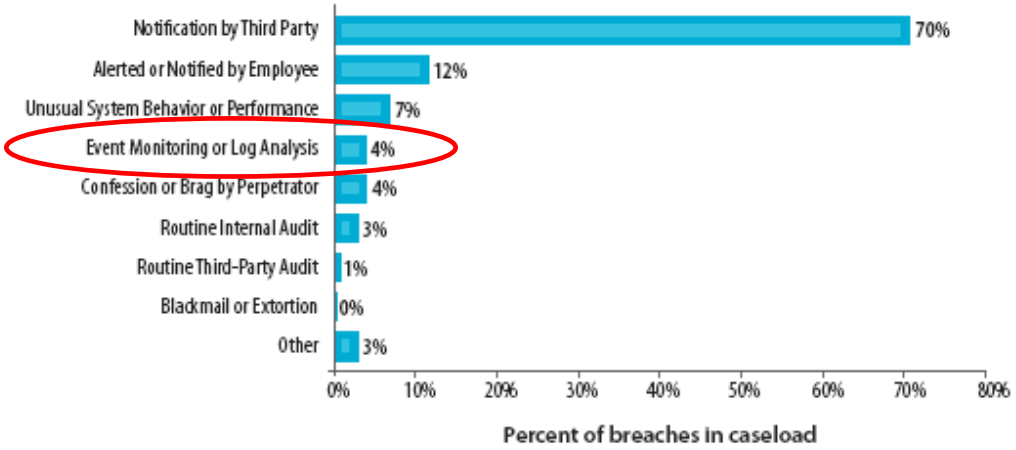
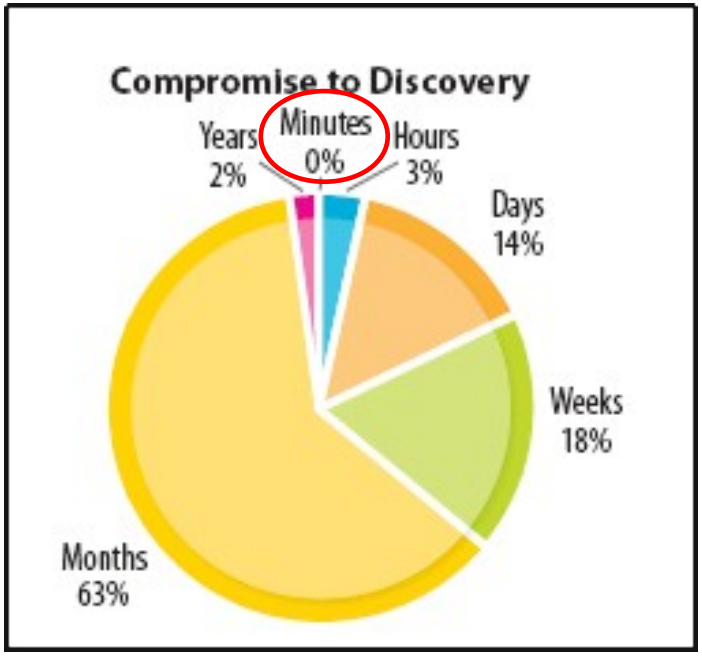
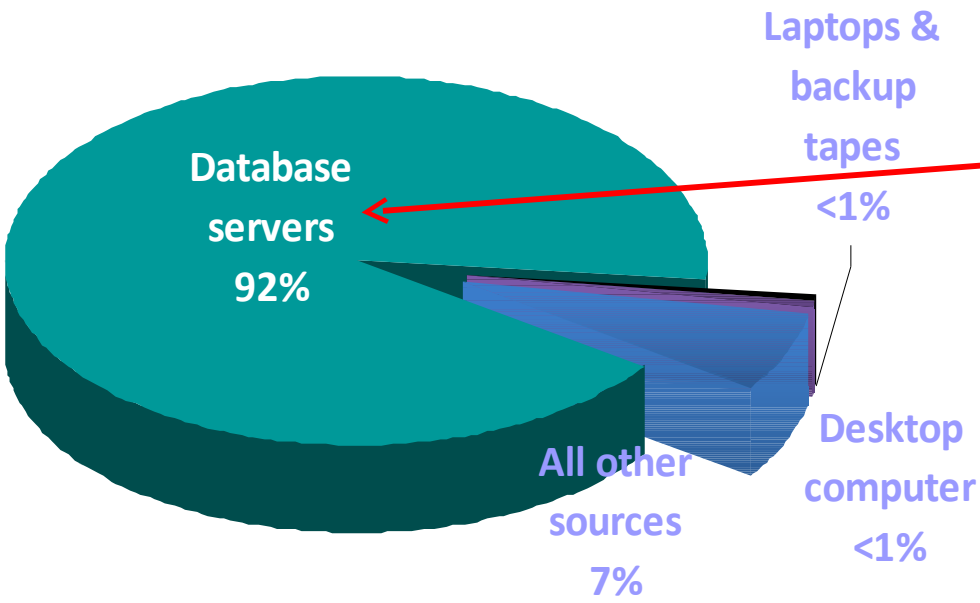


Figure 22. Data Breach Discovery Methods



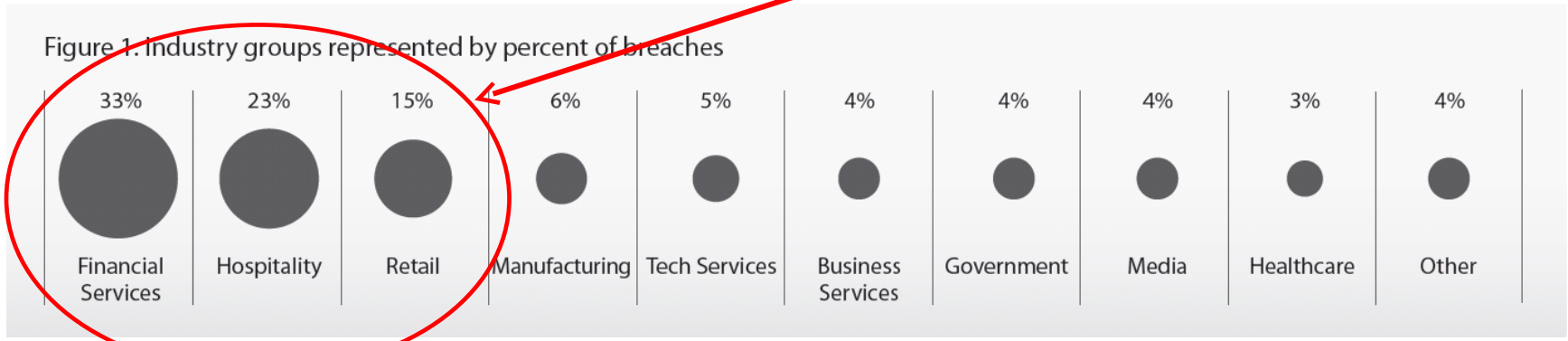
Adatvesztés, adatszivárgás forrásai és érintett területek (2010)

http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf

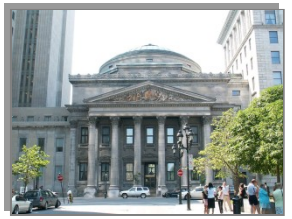


2009-ben ez az érték 75% volt

A három fő iparág érintettsége 71%



Fő üzleti mozgatórugók a pénzügyi szektorban



- SOX
  - üzleti adatok védelme a jogosulatlan változtatásokkal szemben (ERP, pénzügyi rendszerek, …)
- PCI
  - kártyatulajdonos adataihoz történő hozzáférés követése és ellenőrzése (Req.10)
  - kártyatulajdonos adataihoz biztonságos tárolása (Req. 3)
  - Frissítetlen (unpatched) rendszerek azonosítása, és a frissítések érvényesítése, ellenőrzése (Req. 6)
- Ügyfél adatok megőrzése
  - védelem a 'cyber' csalások és személyazonosító adatok eltulajdonítása ellen
  - személyes adatok megtekintése elleni védelem különösen a kiváltságos felhasználók részéről (DBA, fejlesztők, külső szereplők, ...)

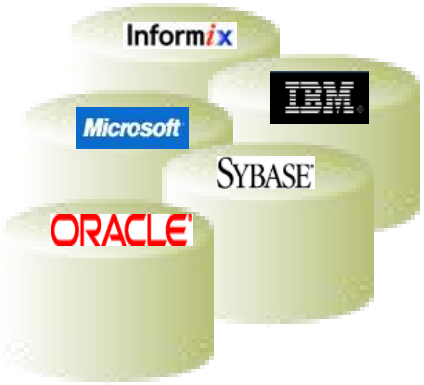
Audit Requirements	COBIT (SOX)	PCI-DSS	ISO 27002	Data Privacy & Protection Laws	NIST SP 800-53 (FISMA)
1. Access to Sensitive Data (Successful/Failed SELECTs)		✓	✓	✓	✓
2. Schema Changes (DDL) (Create/Drop/Alter Tables, etc.)	✓	✓	✓	✓	✓
3. Data Changes (DML) (Insert, Update, Delete)	✓		✓		
4. Security Exceptions (Failed logins, SQL errors, etc.)	✓	✓	✓	✓	✓
5. Accounts, Roles & Permissions (DCL) (GRANT, REVOKE)	✓	✓	✓	✓	✓

DDL = Data Definition Language (aka schema changes)
DML = Data Manipulation Language (data value changes)
DCL = Data Control Language

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

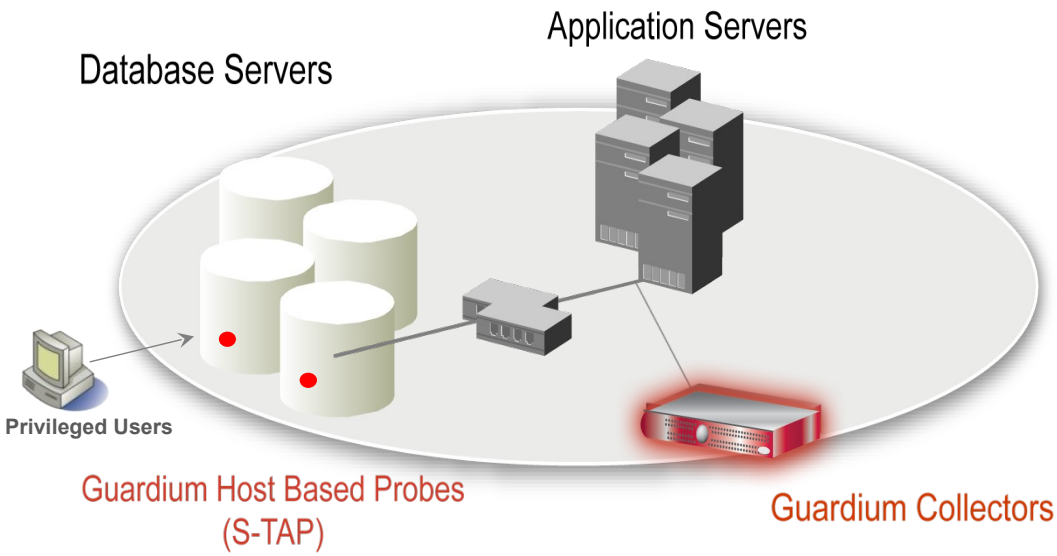
Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY



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

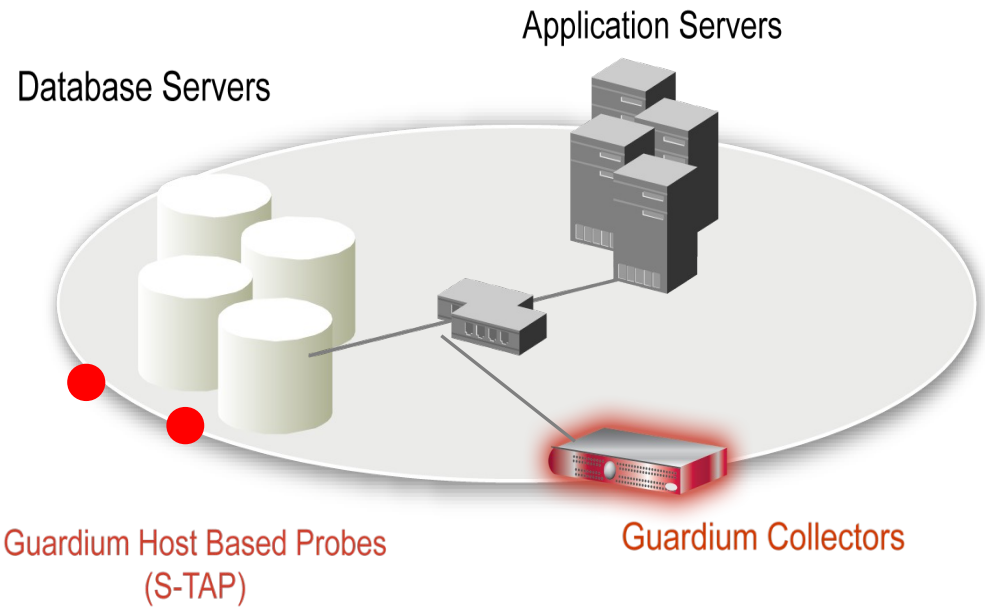


- Teljekörű hozzáférés-monitorozás
- Használatához nem szükséges adatbázis vagy alkalmazás módosítás
- Minimális adatbázis-teljesítmény terhelés
- Egyértelműen elkülöníthető szerepkörök (biztonságos audit állományok)

- 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.)

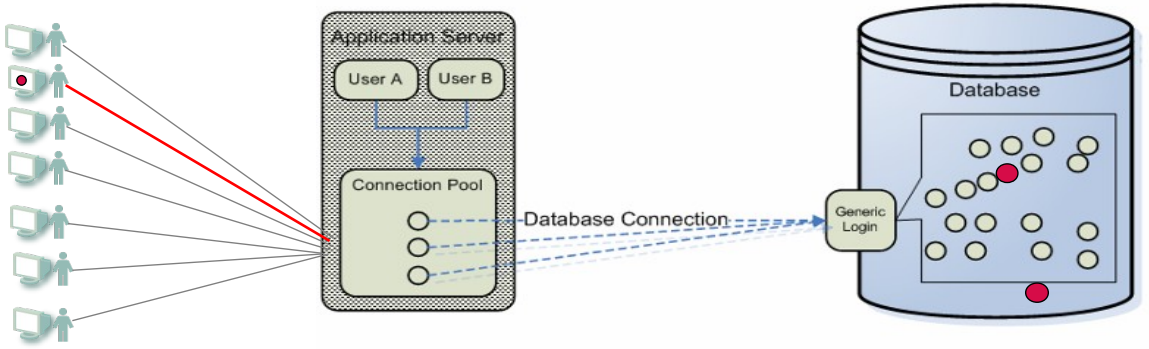
Guardium monitorozási képességek

- 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



Sebezhetőség vizsgálat – valós példa

IBM® InfoSphere™ Guardian®

Results for Security Assessment: [redacted]

Assessment executed 2011-02-03 14:14:14.0
From: 2011-02-02 14:14:14.0
To: 2011-02-03 14:14:14.0
Client IP or IP subnet: Any
Server IP or IP subnet: Any

-- Select a result --

Download PDF

Teszteredmény
100% a legjobb elérhető érték

Tests passing: 13%*

*Percentage does not take into account any current filtering

Based on the tests performed under this assessment, data access of the defined database environments requires significant improvement across a number of areas. Refer to the recommendations of the individual tests to learn how you can address problems within your environment, focusing on severe issues first. Continue running repeats of this assessment with every issue you address to track improvement.

View log
Jump to Datasource list

Összesítés a vizsgált 267 teszt eset alapján
Az egyes tesztek külön csoportba vannak osztva, külön láthatók az eredmények

Result Summary — *Showing 263 of 263 results (0 filtered)*

	Critical			Major			Minor			Caution			Info
Privilege	7p	16f	--	1p	6f	--	--	1f	--	--	--	--	--	1e
Authentication	1p	5f	--	1p	1f	--	--	--	--	--	--	--	--	--
Configuration	2p	2f	--	11p	125f	70e	1p	2f	2e	--	6f	--	--	--
Version	--	--	--	1p	1f	--	--	--	--	--	--	--	--	--
Other	--	--	--	--	--	--	--	--	--	--	--	--	--	--

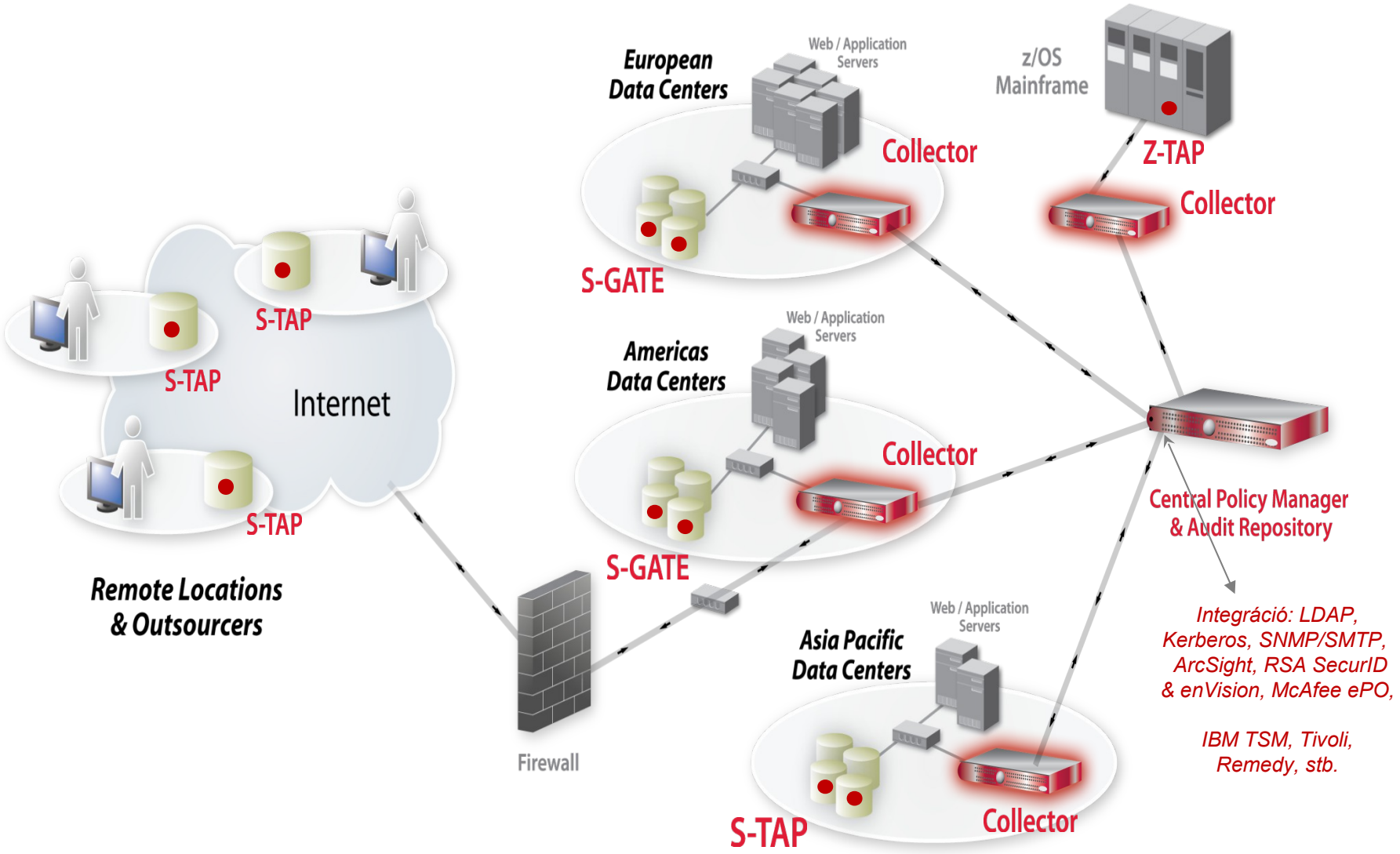
Current filtering applied:
Test Severities: - *Show All* -
Datasource Severities: - *Show All* -
Scores: - *Show All* -
Types: - *Show All* -

Reset Filtering
Filter / Sort Controls

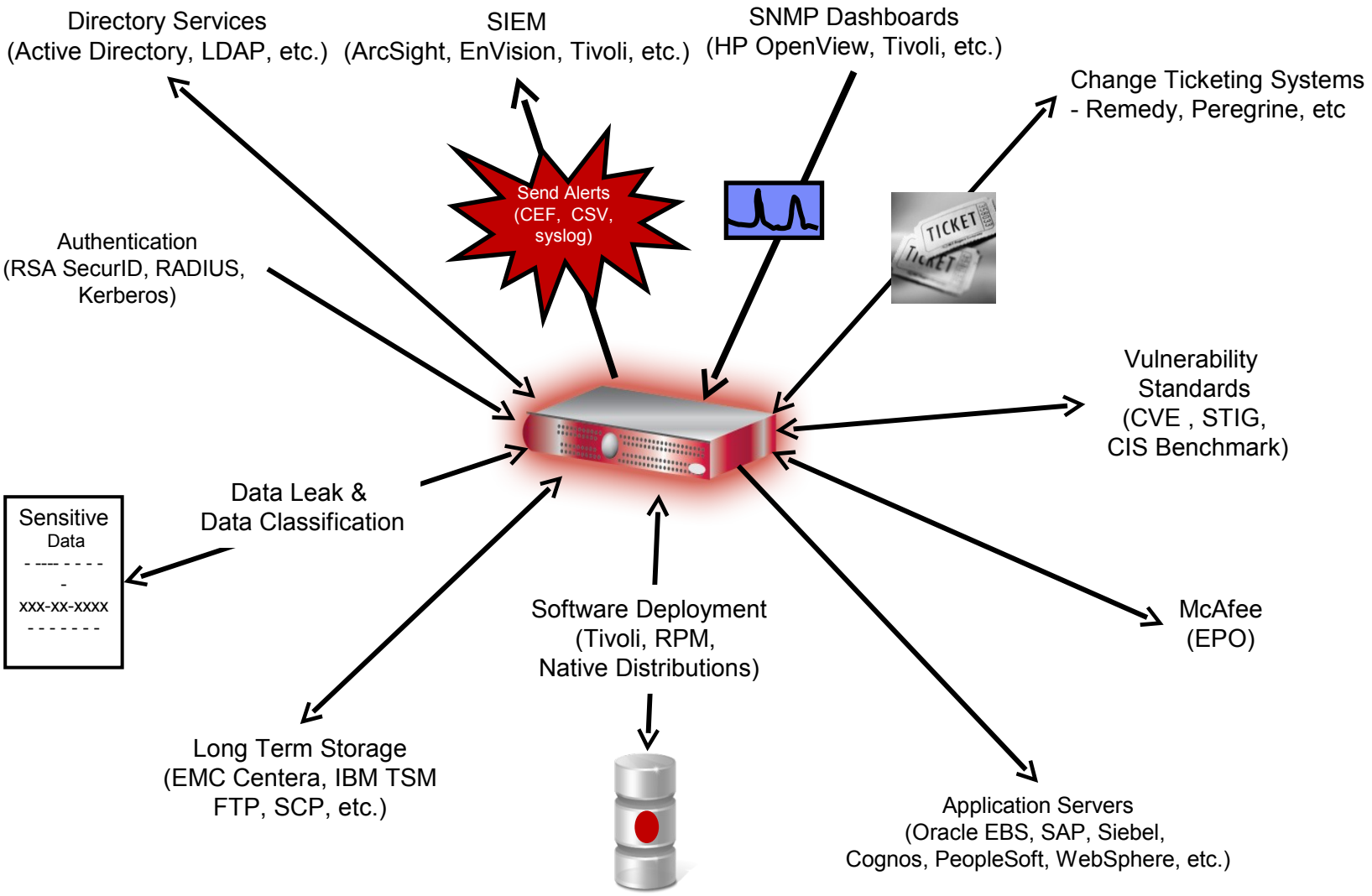
Assessment Test Results — Compare with other results — *Showing 263 of 263 results (0 filtered)*

Test / Datasource	Result
DBA Profile PASSWORD_LIFE_TIME Is Limited Test category: **Conf.** Severity: **Critical** This test checks the value of the PASSWORD_LIFE_TIME parameter. The PASSWORD_LIFE_TIME value serves as a limit to the number of days until a password expires. Setting this value ensures that users are change their passwords at specified	Fail User profile [DEFAULT] setup parameter PASSWORD_LIFE_TIME found out of defined threshold value ***Recommendation:*** *The PASSWORD_LIFE_TIME parameter is not set, allowing users to retain the same password indefinitely. Passwords that have been in use for long periods of time ar likely to become known to unauthorized users. We recommend that you set this parameter in order to limit the lifetime of users' passwords.*

Skálázható, heterogén architektúra



Integráció a meglévő infrastruktúrával a költséghatékonyság érdekében

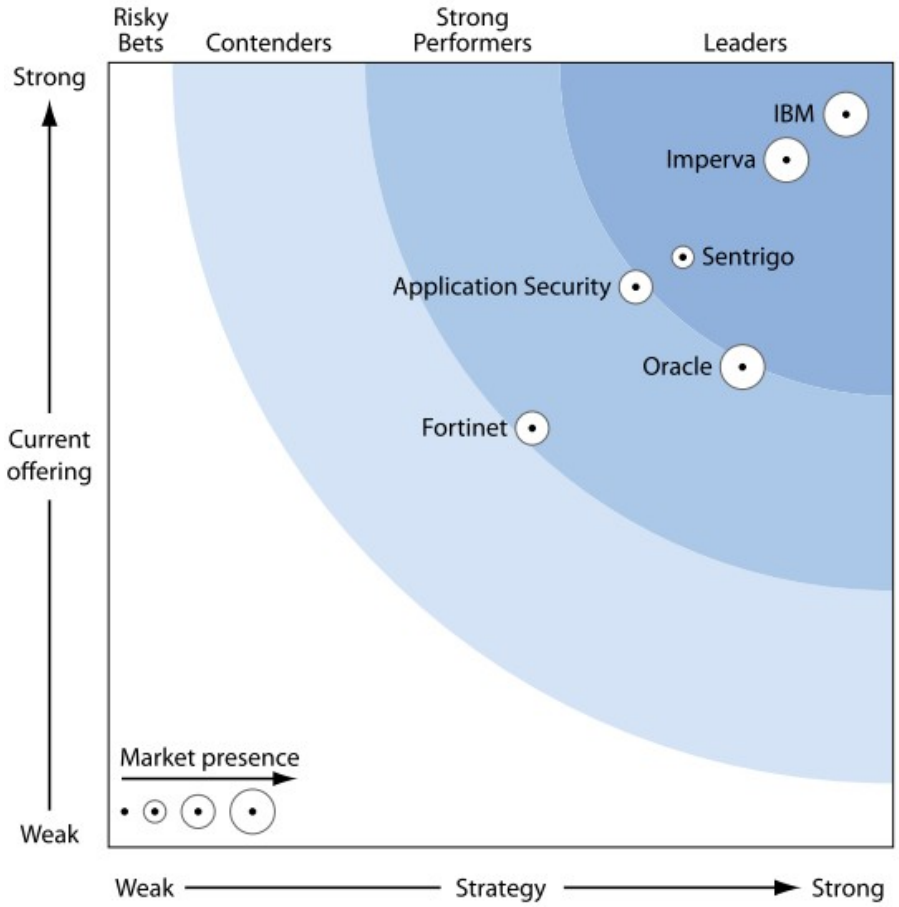


Az üzleti élet java használja....

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