Filip Uram – Information Management Sales Leader

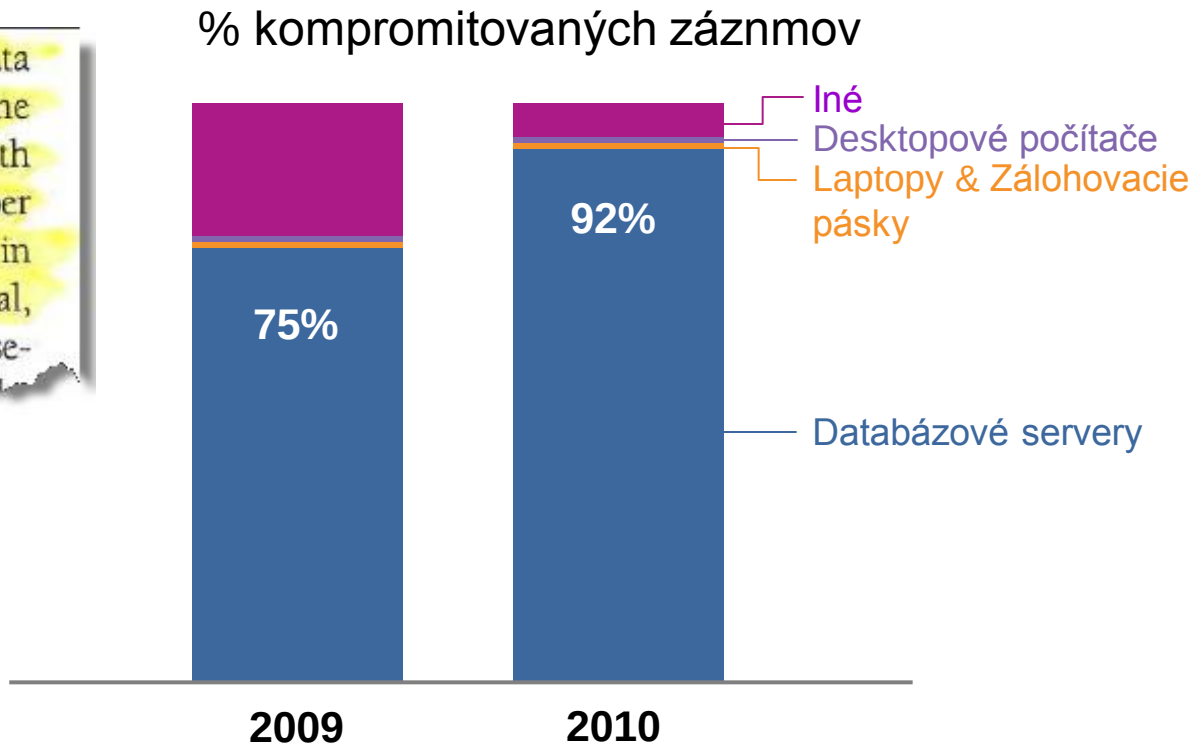
Technické prostriedky ochrany informácii v databázach

Document number

Databázove servery sú primárnym zdrojom úniku dát

For example, the 2010 Verizon data breach report places databases as the top type of compromised asset by both the number of breaches and the number of records stolen. Yet our investments in protecting database systems is minimal, at best. When it comes to database se-

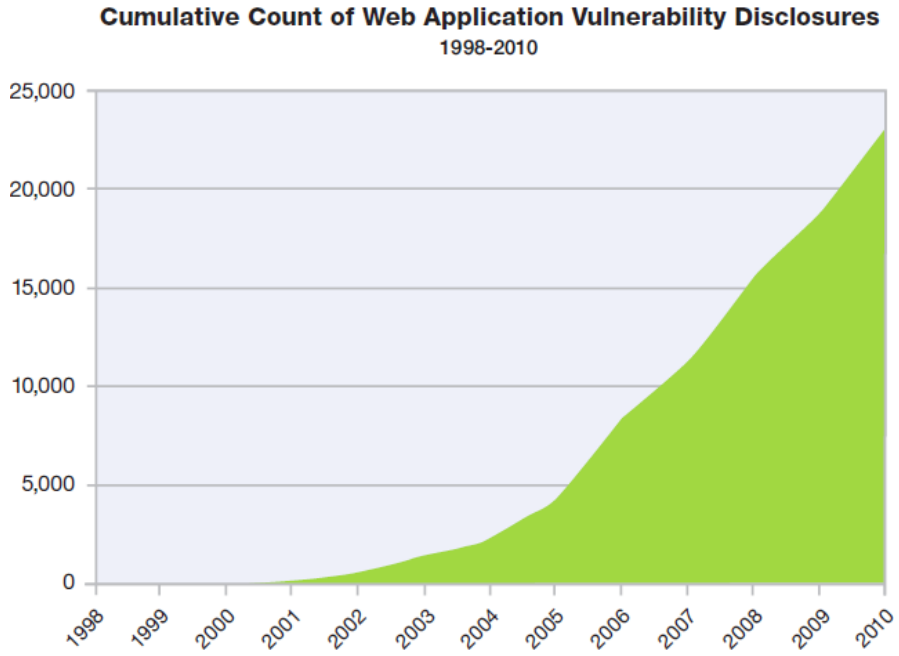
InformationWeek
"Epic Fail"
10/11/2010

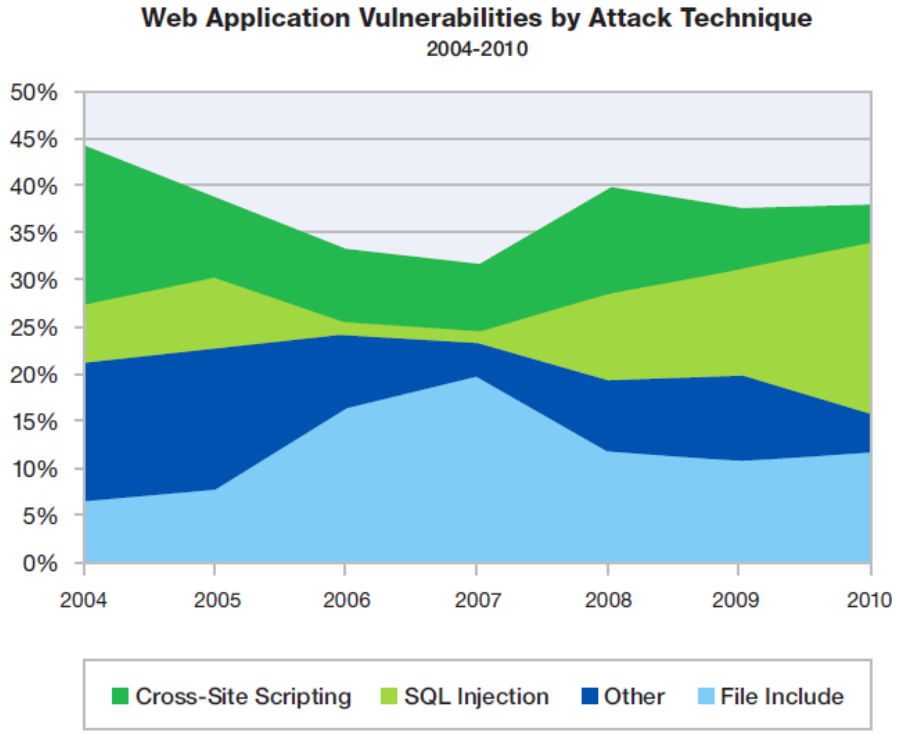


Sources: Verizon Business Data Breach Investigations Report 2009, 2010
www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf

"Aj keď veľká pozornosť je venovaná offline dátam, mobilným a koncovým zariadeniam, tieto nie sú primárnym zdrojom úniku dát.."

Počet zraniteľností webových aplikácii kontinuálne rastie





"Väčšina webových aplikácii je produktom zákazkového vývoja … Celkový počet zraniteľností je zásadne vyšší ako ten, o ktorom je odborná verejnosť informovaná. … Bezpečnostné problémy webových aplikácii prevyšuje počet všetkých ostatných zraniteľností na Internete.

Zdroj: IBM Security Solutions X-Force® 2010 Trend and Risk Report
www.ibm.com/security/xforce

Príklady útokov zo sveta

- Spoločnosť SONY sa stala terčom útoku, pri ktorom hackeri získali prístup k osobným údajom 77 miliónov užívateľov, 23.400 kreditných kariet. Celkové náklady sa vyšplhali na 170 miliónov USD

- Zamestnanec spoločnosti zabezpečujúcej predaj lístkov na Majstrovstvá sveta vo futbale v rokoch 2006 a 2010 spreneveril údaje o viac ako 250.000 klientoch vrátane dátumu narodenia, čísla pasu a podobne.

- Podnikanie spoločnosti Citibank v juhovýchodnej ázii bolo lokálnymi regulátormi zásadne obmedzené po tom, ako jeden zo zamestnancov zneužil údaje o zákazníkoch a ich kreditných kartách.

Príklady vnútorných hrozieb z reálneho sveta

- **Neautorizované zmeny dát, porušovanie interných predpisov**
  - Zmena vnútorných výkazov
  - Pochybenia administrátorov pri prevádzke IT
- **Krádež citlivých dát**
  - Telekomunikačné tajomstvo
  - Obchodné tajomstvo
  - Osobné údaje
- **Interný fraud**
  - Hypotekárna kalkulačka: úprava výpočtu modelu
  - Predplatné karty mobilných operátorov: podvodné navýšenie kreditu
  - Poskytovatelia energii: zníženie reálneho stavu spotreby
  - Poskytovatelia zdravotnej starostlivosti: fiktívne výkony na účet zdravotných poisťovní

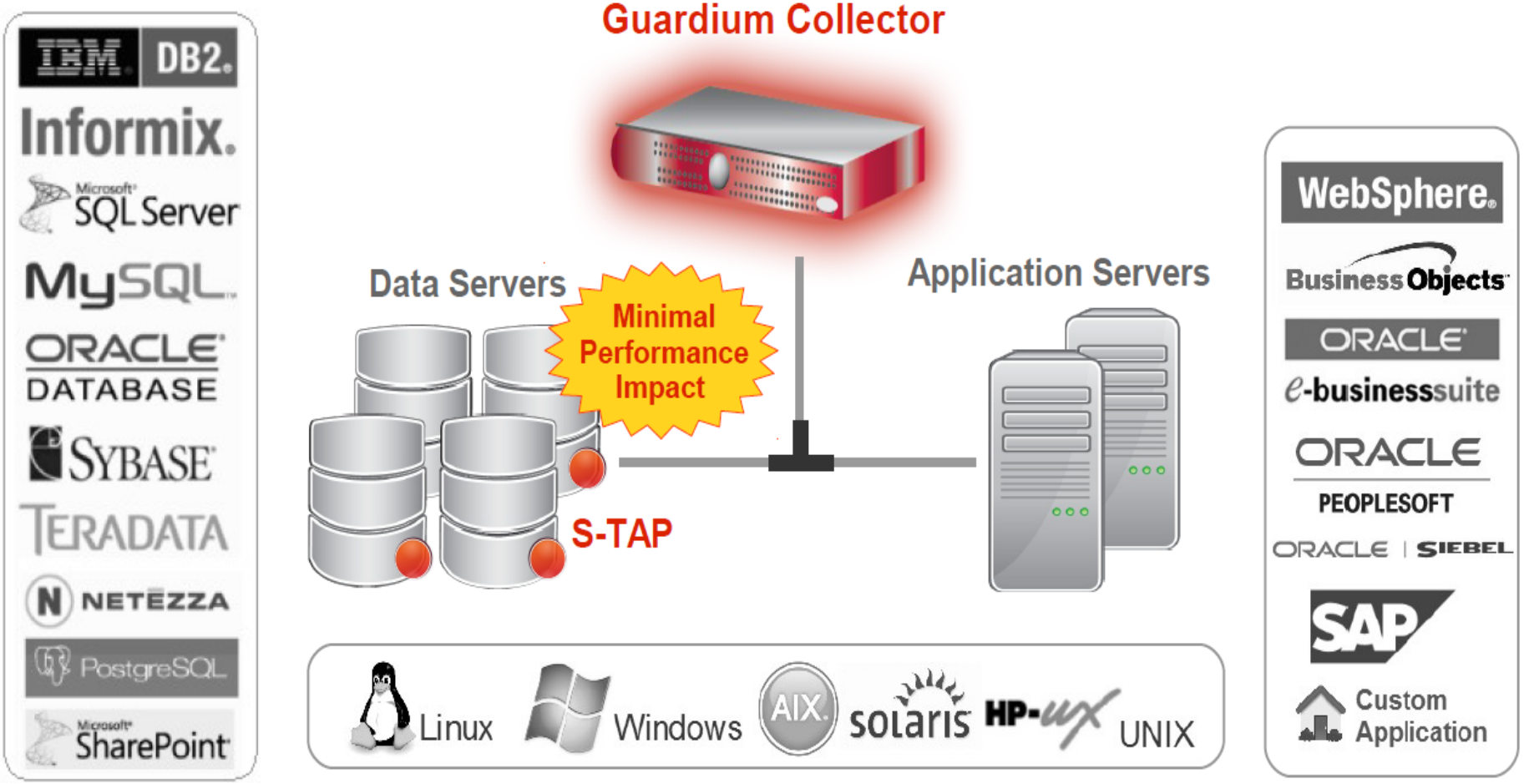
Čo je Guardium ?

- Spoločnosť Guardium bola založená v roku 2002 na MIT ako reakcia na dopyt na trhu po bankrote spoločnosti Enron
- V súčasnej dobe používa Guardium viac ako 400 zákazníkov po celom svete
- Z finančného sektoru sú to napríklad Citibank, Bank of America, HSBC, ING, UniCredit, Societe Generale, Allianz
- Od roku 2009 sú produkty pod názvom *InfoSphere Guardium* súčasťou IBM Integrated Data Management portfólia

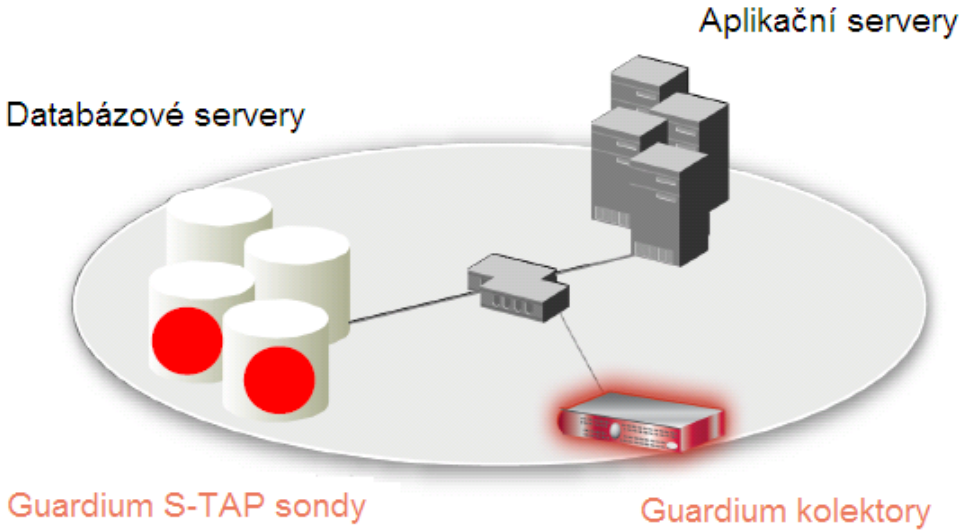
Čo robí Guardium ?

- Monitorovanie zabezpečenia databázy
- Monitorovanie databázovej prevádzky v reálnom čase a zamedzenie prístupu k citlivým dátam
- Rýchle zistenie neautorizovaných alebo podozrivých aktivít na základe definovaných pravidiel a politík
- Automatizované workflow pre efektívnu nápravu skutočností, ktoré sú v rozpore s požiadavkami bezpečnostných štandardov
- Jednotné prostredie pre správu väčšiny databázových platforiem a aplikačných prostredí:
  - Informix, DB2, Oracle, SQL Server, z / OS, Sybase a ďalšie
  - SAP, Siebel, Oracle EBS, PeopleSoft, WebSphere a ďalšie

Architektúra Guardium



Ako funguje Guardium?



- 100% viditelnosť všetkých databázových operácii vrátane lokálneho prístupu
- Nevyžaduje žiadne zmeny v konfigurácii databázového systému alebo v aplikácii
- Minimálny vplyv na výkonnosť databázy

- Oddelenie úloh so zabezpečeným úložiskom auditných informácií
- Politiky a pravidla poskytujúce dostatočne granulárne monitorovanie a audit informácii „*kto*, *čo*, *kedy* a *ako*“ o každej činnosti
- Automatický systém varovania v reálnom čase

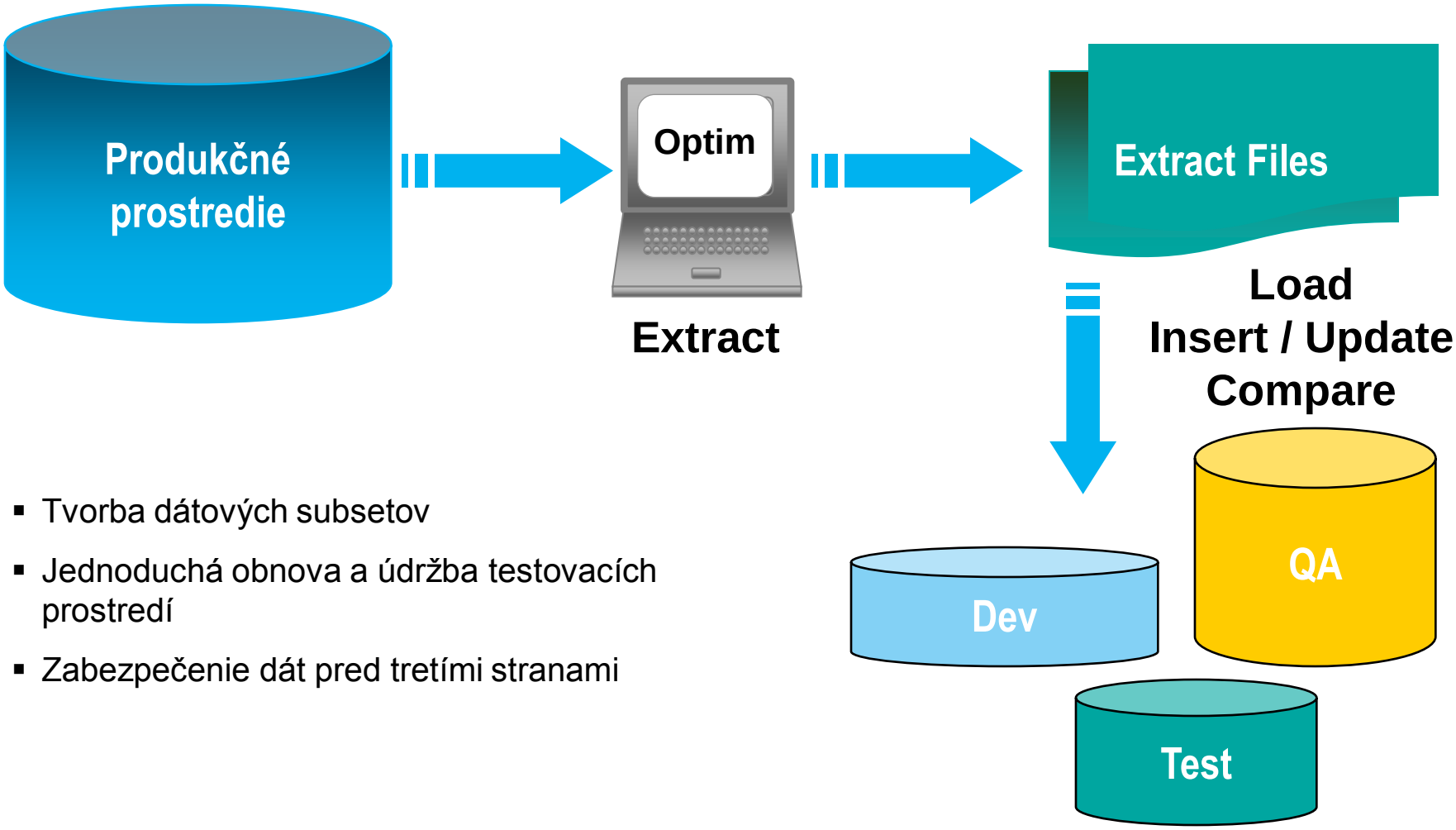
Čo InfoSphere Guardium monitoruje ?

- SQL chyby a neúspešné prihlásenia
- DDL príkazy (Create/Drop/Alter Tables)
- SELECT dotazy
- DML príkazy (Insert, Update, Delete)
- DCL príkazy (Grant, Revoke)
- Uložené procedúry
- XML spracovávané databázami
- Data (záznamy) vrátené databázovým systémom späť uživateľom

Výhody oproti konkurencii

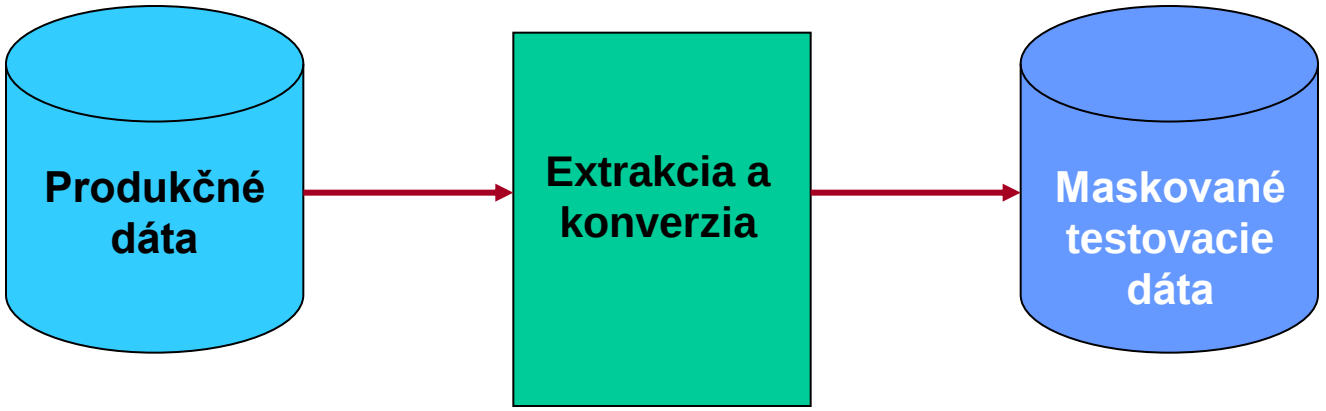
- Úplne nezávislé na systéme natívneho databázového auditu
- Integrácia s existujúcimi systémami (napr. priama integrácia s LDAP, QRadar, archivácia do TSM atď.)
- Agregácia a korelácia dát z rôznych systémov v reálnom čase
- Efektívny spôsob ukladania auditných dát
- Aj po archivácii dát z kolektora sú dáta stále dostupné
- S-TAP sonda a aktívne opatrenia (S-GATE)
- Komplexný prístup k vyhodnoteniu zraniteľnosti systému s preddefinovanými pravidlami
- Automatizovaná aktualizácia sledovaných objektov
- Zjednodušená konfigurácia prostredníctvom GuardAPI rozhrania
- Optimalizácia sieťovej komunikácie filtrovaním údajov potrebných iba pre audit
- Zabudovaný workflow proces pre riešenie incidentov

Optim™ Test Data Management



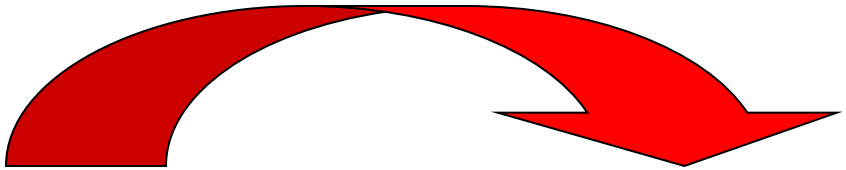
- Tvorba dátových subsetov
- Jednoduchá obnova a údržba testovacích prostredí
- Zabezpečenie dát pred tretími stranami

Maskovanie dát s Optim riešením



Transformuje citlivé dáta počas migrácie z produkčných do testovacích prostredí

Maskovanie je transparentné voči okolitému svetu



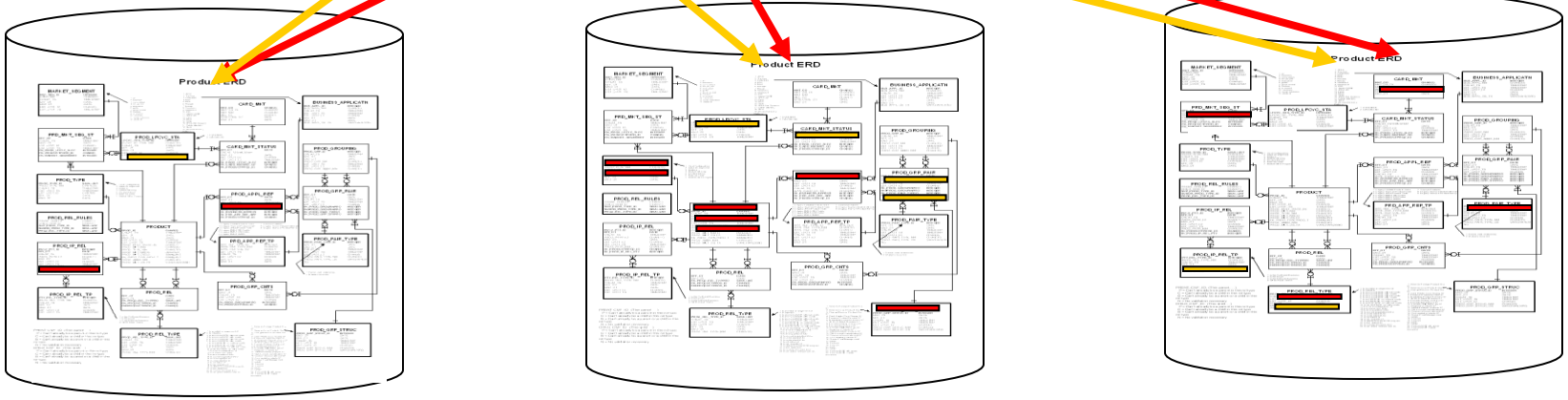
Pôvodné dáta

Po zamaskovaní

Určenie citlivých dát je netriviálna úloha

Sensitive Data Repository

Row	Member	SS #	Age	Phone	Sex
1	595846226	123-45-6789	15	(123) 456-7890	M
2	567472596	138-27-1604	8	(138) 271-6037	F
3	540450091	154-86-4196	22	(154) 864-1961	M
4	514714372	173-44-7900	55	(173) 447-8996	F
5	490204164	194-26-1648	4	(194) 261-6476	F
6	466861109	217-57-3046	66	(217) 573-0453	M
987,623	444629628	243-68-1812	25	(243) 681-8107	F
987,624	423456789	272-92-3629	87	(272) 923-6280	M



- Nájdenie citlivých dát v jednom systéme môže trvať dni
- Celkové aj čiastočné citlivé dáta sa nachádzajú v stovkách polí a tabuliek

Citlivé údaje zvyknú byť skryté

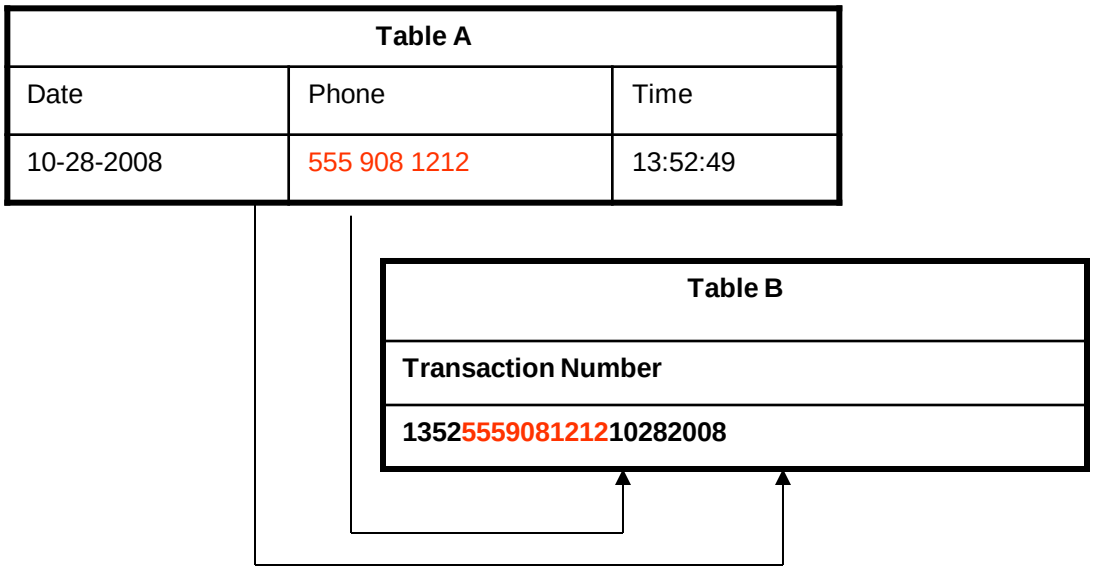
- Citlivé dáta nie je vždy možné nájsť pomocou jednoduchých table scanov
  - Je potrebné spojiť tabuľky a vyhľadávacie tabuľky
  - Skryté ako súčasť väčších reťazcov
  - Skryté naprieč poľami

- Korporátna „pamäť" je krátka
  - Nekompletná dokumentácia
  - Špecialisti a dátoví analytici poznajú väčšinou len jeden maximálne dva systémy

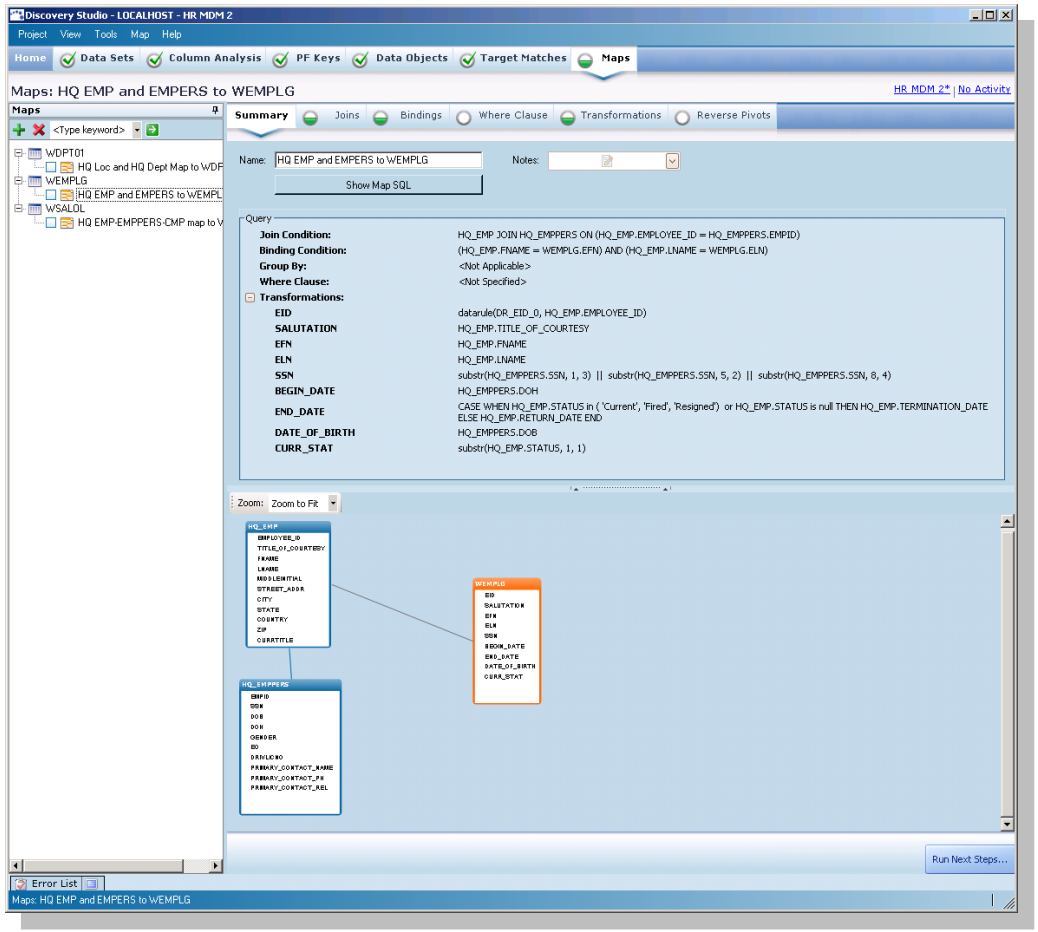
- Stovky tabuliek a milióny riadkov
  - Komplexné
  - Ťažko verifikovateľné

- Problémy s dátovou kvalitou otázky

identifikácie citlivých dát ešte viac komplikujú



IBM InfoSphere Discovery nájde aj skryté citlivé dáta



- Automatizovanie vytvorenie dátového modelu
- Zisťovanie vzájomných väzieb medzi dátami
- Určenie citlivých dát, ktoré potrebujú byť chránené