RECRO net
We know IT

HROUG

Nadzor i zaštita baza u stvarnom vremenu

Rovinj, 19.-23.10.2010.

Nevenko Bartolinčić

CISCO PARTNER Gold Certified

Microsoft GOLD CERTIFIED Partner

CISCO PARTNER Learning

Raspored

- Sigurnost baza podataka u 2010
- Guardium DAM
- Poslovne primjene
- Razno

Stanje sigurnosti baza podataka u 2010. godini

1. Zaštita povjerljivih informacija unutar baza podataka nije više samo dobra sigurnosna praksa već nužnost za svaku tvrtku.

2. Razina prijetnji danas je iznimno visoka, kako internih tako i eksternih, od zlonamjernih napača do nezadovoljnih djelatnika.

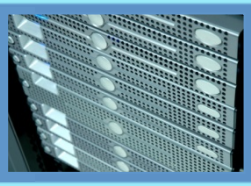
3. Tvrtke su stavljene pred zid zahtjeva za zaštitu informacija, privatnosti, ali i zakonske sukladnost – zahtjev učinkovitosti, ali i automatiziranja.

Uobičajene brige na razini CSO-a u 2010. godini

Gdje se nalaze moje povjerljive informacije i tko im pristupa?

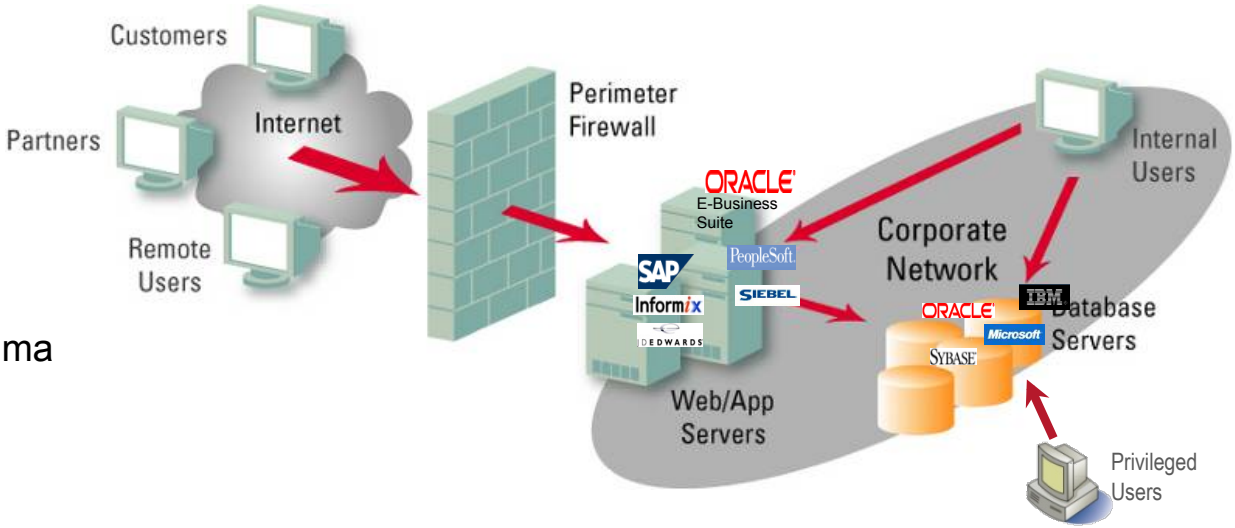
Kako mogu provesti pravila pristupa i izmjena nad kritičnim informacijama?

Kako mogu provjeriti stanje baza podataka, ranjivosti i upravljati konfiguracijom?



Kako mogu automatizirati izvještavanje i biti sukladan sa zakonskom regulativom?

Sigurnost baza podataka - izazovi



Kompleksna infrastruktura

- Heterogena
- Podložna čestim izmjenama

Različiti načini pristupa

- Aplikacije putem mreže
- Eksterni pristup
- Lokalni, privilegirani pristup

Performanse sustava su imperativ

- Sustavi od velike važnosti za poslovanje
- Nevoljke izmjene i ‘dorade’

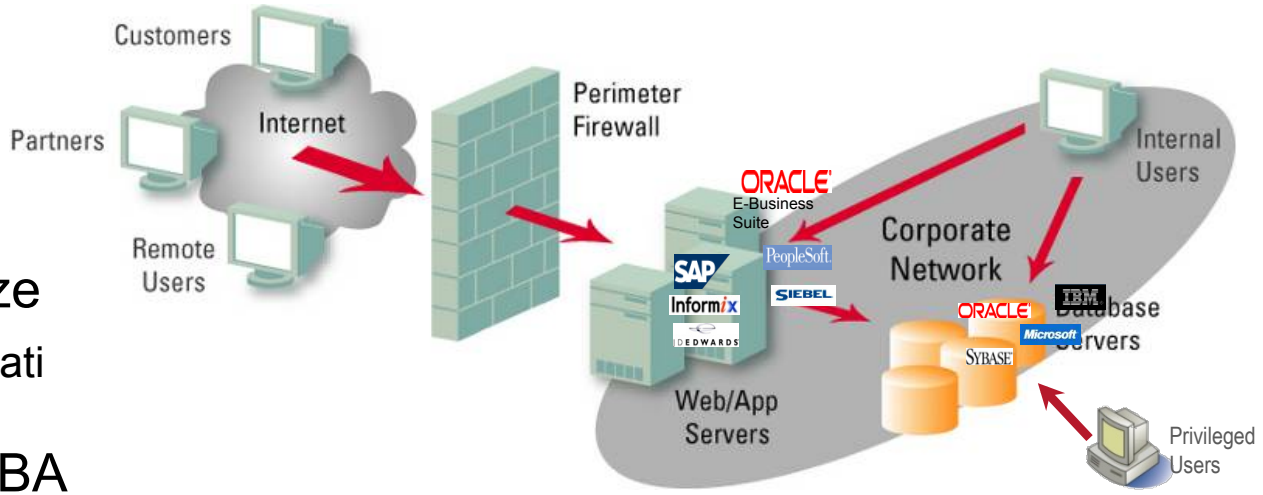
Dijeljene odgovornosti

- Tim za infrastrukturu i tim za baze podataka
- Sigurnost i zakonska sukladnost

Prijetnje u porastu

- Interne i eksterne

Tradicionalno logiranje i nadgledanje baza



Alati koji dolaze uz baze

- Dodatno razvijeni alati

Upravljani od strane DBA

- Sigurnost je niskog prioriteta
- Fokus na performanse sustava
- Neometan pristup
- “Povjerenje” kao temeljni faktor rada

“Daleko od savršenosti ali bez alternative”

- Uvjerenje da nije moguće postići bolju vidljivost nad sustavom i dobre performanse – stvar kompromisa?

Separation of Duties – upravljanje DBA

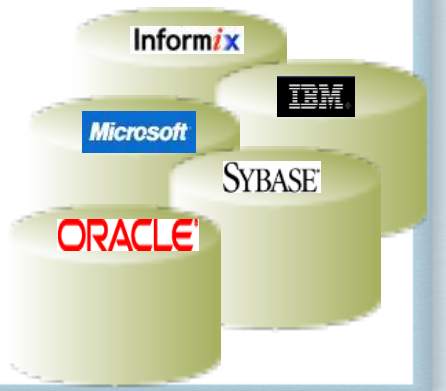
Bitno je imati strategiju upravljanja privilegiranim korisnicima posebice vezano uz aktivnosti kreiranja, izmjena ili brisanja...

- **Korisničkih računa** – jedan administrator ne smije moći kreirati korisnika i raditi promjene njegovog profila
- **Privilegija** – pravo dodjela privilegija i manipuliranja istima ne smije biti u rukama jedne osobe
- **Lozinki** – jedna osoba ne smije imati pristup kreiranju, izmjenama i upravljanja lozinikama
- **Strukture baza**– fundamentalne promjene nad strukturom baza mogu imati veliki utjecaj na rad sustava, jedna osoba ne smije moći raditi proizvoljne izmjene
- **Tablica** – promjene nad tablicama moraju biti upravljane i autorizirane
- **Procedura** – promjene procedura mogu imati višestruke posljedice, ova kategorija privilegija mora biti podijeljena među više osoba
- **Funkcija** – privilegija definiranja funkcija unutar baza mora biti nadgledana kako bi izbjeli mogućnost neovlaštenog pristupa ili zloupotrebe informacija

"Ispravna podjela odgovornosti i upravljanje znači da ne postoji niti jedna osoba koja kontrolira sve."

Što nedostaje tradicionalnom logiranju?

1. **Detalji audita**
   - Kontrola privilegiranih korisnika (DBA)
   - Identifikacija korisnika unutar aplikacije
2. **Utječe na performanse sustava**
   - Nije optimalan za sigurnost
   - Povećano opterećenje CPU-a
3. **Različite metode za različite baze**
   - Nedostatak unificiranog pristupa
   - Neučinkovitost, nedostatak sigurnosnog aspekta
4. **Pohrana podataka, izvještavanje i forenzika**
   - Veliki zahtjevi za prostorom za pohranu
   - Ručno izvještavanje i forenzika
5. **Bez zaštite u realnom vremenu**
   - Upozorenje na poremećaje/anomalije sustava
   - Nedostatak mogućnosti blokiranja neovlaštenog pristupa
6. **Bez razdjele odgovornosti/zaduženja**
   - Administratori prezauzeti da razmišljaju o sigurnosti
   - Administratori ne mogu nadgledati sami sebe!



Guardium Database Activity Monitoring

Detaljno nadgledanje i kontrola nad izmjenama

- Nadgleda sav mrežni SQL promet kroz SPAN port ili TAP
- Nadgleda sav lokalni pristup korištenjem agenta na DB serveru
- Kontrola izmjene nad konfiguracijom baza
- Alerting i blokiranje neželjene aktivnosti

Jedno rješenje za heterogena okruženja

- Oracle, MS SQL, IBM DB2, MySQL, itd
- SAP, Oracle EBS, Siebel, kao i druge aplikacije
- Windows, Linux, Solaris, AIX, HP UX, z/OS, itd

Neovisan o Database Management Sistemu

- Ne koristi alate za logiranje na bazama
- Ne degradira performanse sustava
- Ne zahtijeva izmjene ili rad na bazama
- Razdvaja odgovornosti (separation of duties)

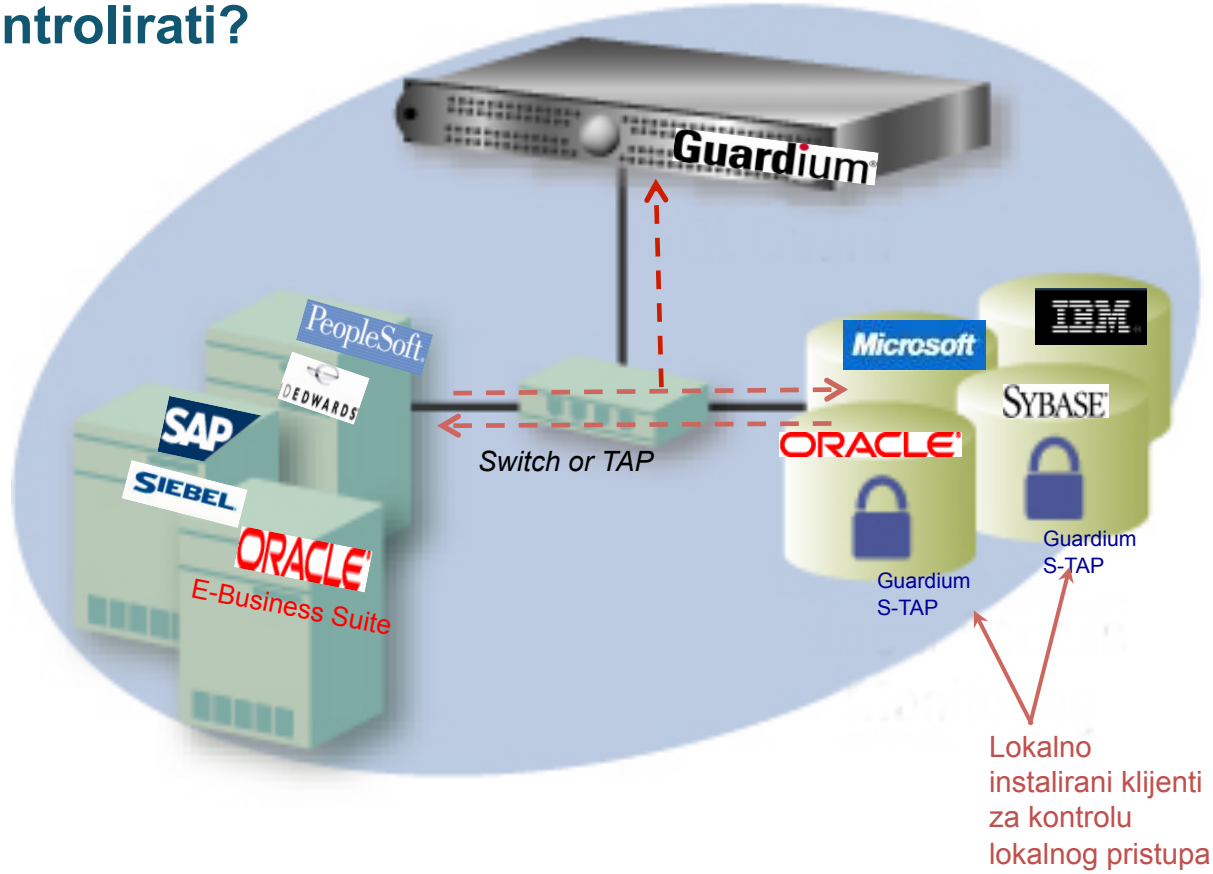
Automatizirano izvještavanje i pohrana

- Predefinirani izvještaji
- Alat za forenziku
- Olakšava postizanje pravne i ine sukladnosti

Detaljno nadgledanje SQL aktivnosti

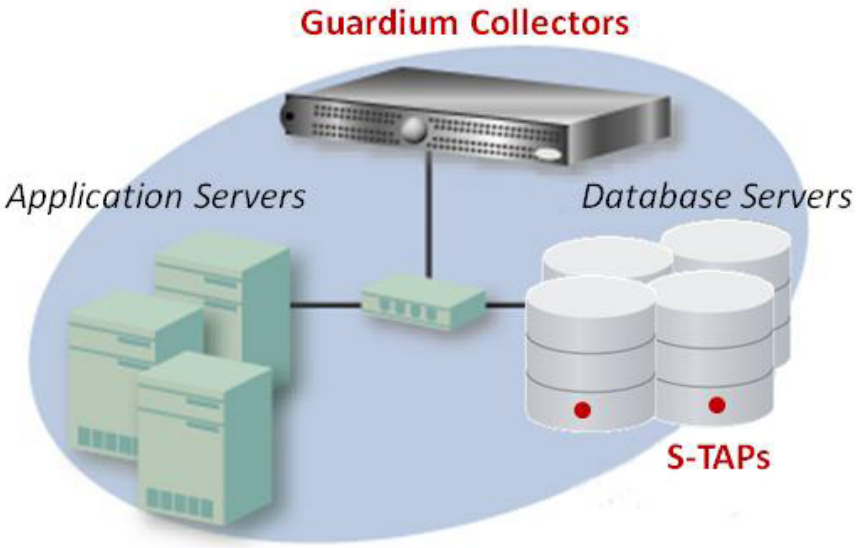
Što Guardium može kontrolirati?

- **SQL greške i krive logine**
- **DDL naredbe**
  (Creat/Drop/Alter Tables)
- **SELECT upite**
- **DML naredbe**
  (Insert, Update, Delete)
- **DCL naredbe**
  (GRANT, REVOKE)
- **Proceduralne jezike**
- **XML datoteke izvršene od strane baze**



S-TAP agent omogućuje kompletnu vidljivost

- Opcionalni, lagani softver koji omogućuje nadgledanje svih aktivnosti na bazi (Unix or Windows).
- Vidi 100% aktivnosti, uključujući TCP, pristup dijeljenoj memoriji, Oracle BEQ, named pipes, TLI, i IPC spajanja
- Ne zahtijeva izmjene na bazi podataka
- Provjereno prikuplja 1000 audit unosa po sekundi, sa manje od 3% učinka po performanse
- S-GATE za kompletnu blokadu spajanja



Nadgledanje aktivnosti korisnika unutar aplikacije

Identifikacija korisnika unutar aplikacije

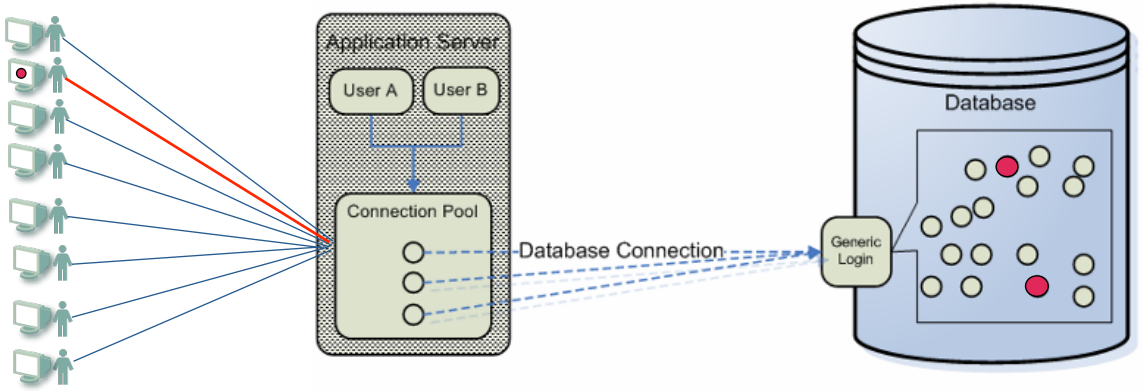
- Otkriva potencijalnu zloupotrebu
- Detaljniji nalazi audita (npr. revizija u financijskim institucijama)

Podržane aplikacije

- Oracle E-Business Suite, PeopleSoft, Business Objects Web Intelligence, JD Edwards, SAP, Siebel, moguće prilagođavanje pojedinoj aplikaciji

Podržane platforme

- IBM WebSphere, BEA WebLogic, Oracle Application Server, Microsoft .NET, JBoss Enterprise Application Platform



Detaljnije izvještavanje

Primjer izvještaja kroz standardne alate:

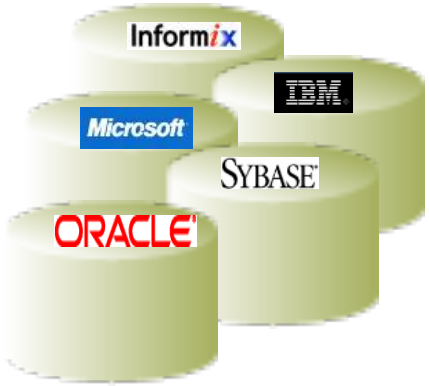
SAP USER requested DATA from CUSTOMER Database and the database returned DATA

Primjer izvještaja korištenjem Guardium rješenja:

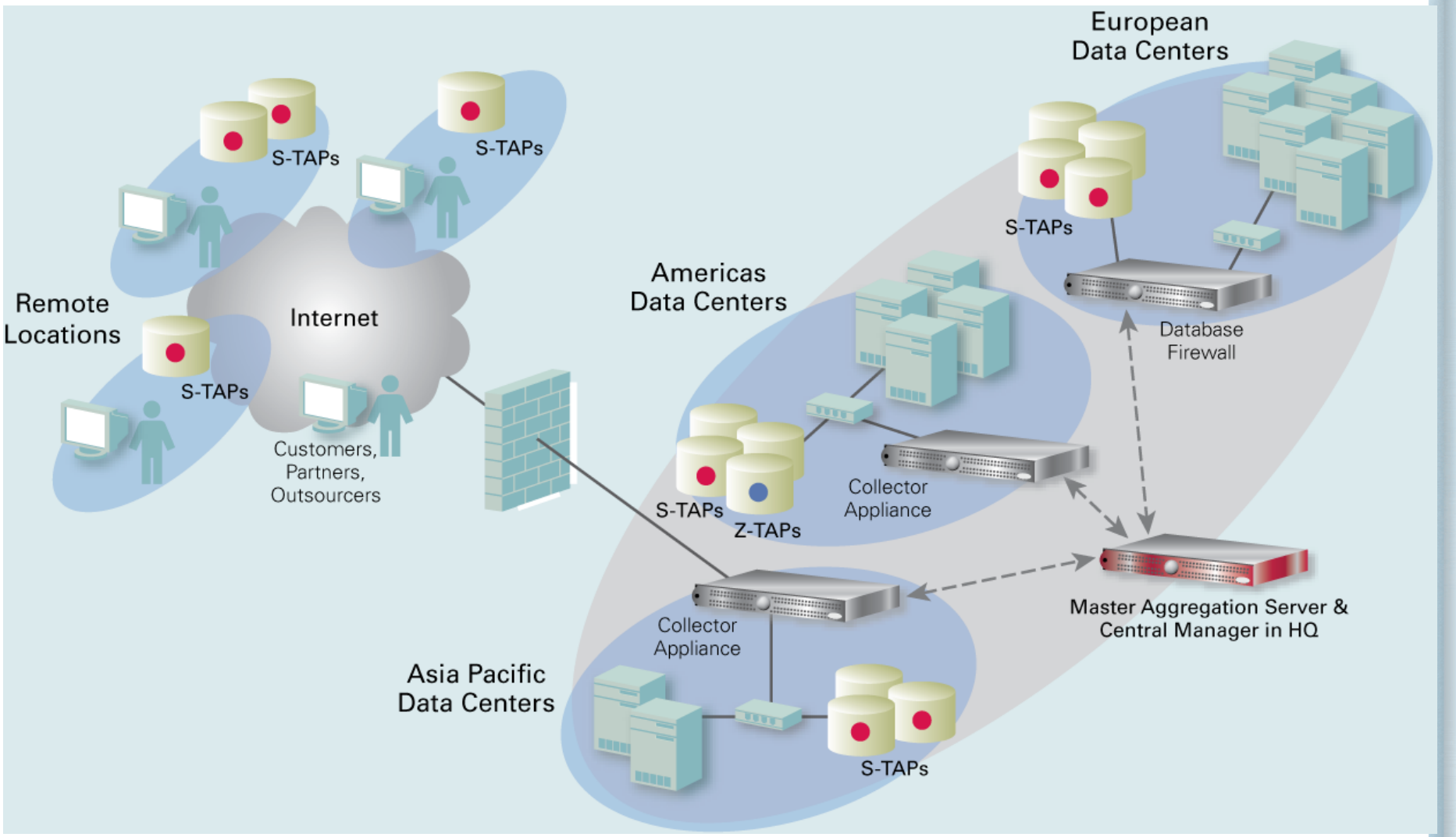
SAP USER, DAVID SMITH, requested FIRST NAMES, LAST NAMES, E-MAIL ADDRESS, CREDIT CARD NUMBERS, for ALL accounts from CUSTOMER database and the database returned 349271 records

Osiguranje konfiguracije kroz Change Auditing System

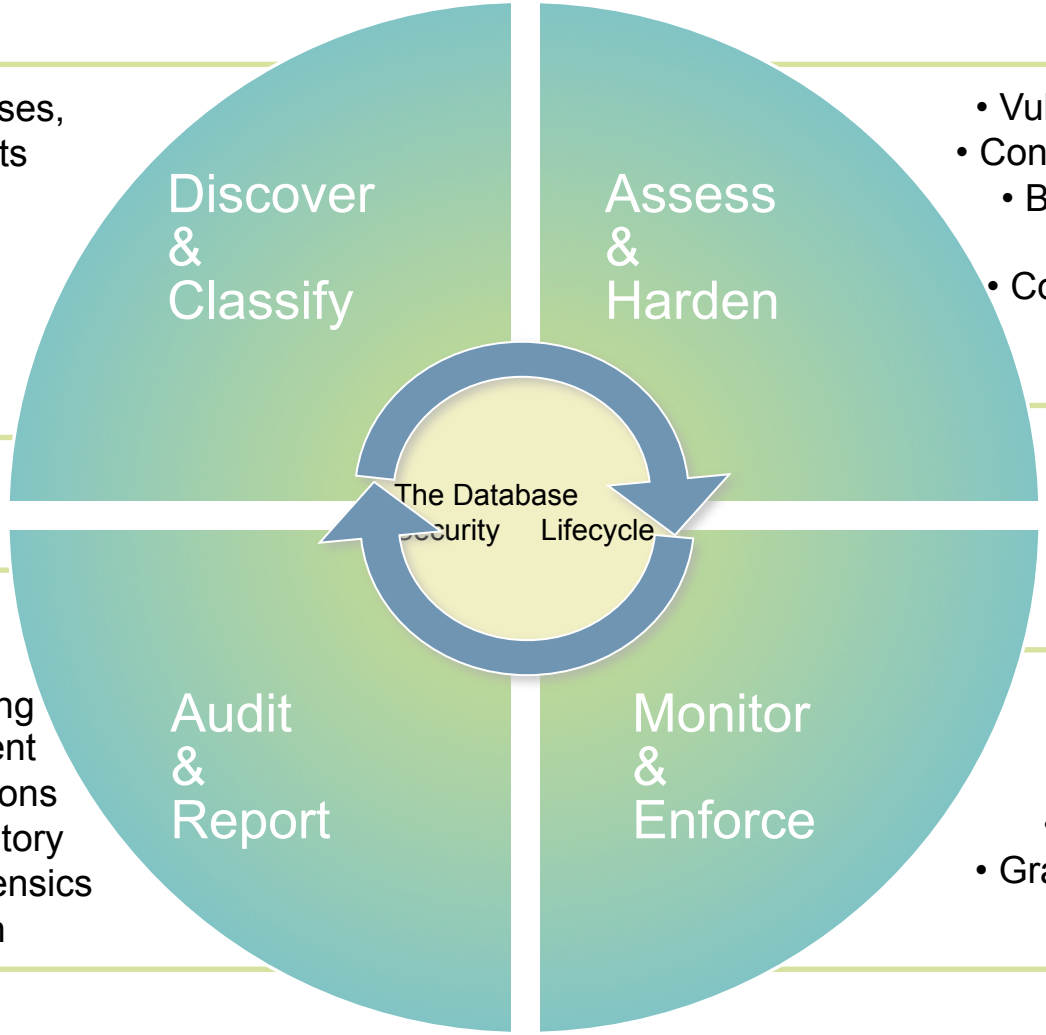
- Nadgledanje i izvještavanje o svim promjenama naspram standardne (definirane) konfiguracije
- Omogućuje zaključavanje sustava od ikakvih izmjena
- Prati izmjene na razini OS-a, poput:
  - Datoteka i checksuma
  - Skripti
  - Varijabli okruženja
  - Postavki unutar registry-a
- Prati promjene na razini SQL baze:
  - SQL statements
  - SQL scripts



Skalabilna višeslojna arhitektura



Puni krug zaštite baza podataka



- Discover all databases, applications & clients
- Discover & classify sensitive data

- Vulnerability assessment
- Configuration assessment
- Behavioral assessment
- Baselining
- Configuration lock-down & change tracking
- Encryption

- Centralized governance
- Compliance reporting
- Sign-off management
- Automated escalations
- Secure audit repository
- Data mining for forensics
- Long-term retention

- 100% visibility
- Policy-based actions
- Anomaly detection
- Real-time prevention
- Granular access controls

Poslovne primjene

Financijske institucije:

- Separation of duties
- Izvješća sukladno zahtjevima revizije

Državne institucije:

- Zaštita privatnosti
- Separation of duties

Telekomi

- Zaštita privatnosti (CR-a)

Ostale tvrtke:

- Zaštita intelektualnog vlasništva

Hvala!

Pitanja ???

RECRO-NET d.o.o.	http://www.recro-net.hr
Av. V. Holjevca 40	Tel: +385 1 3030 600
10010 Zagreb	Fax: +385 1 6699 500
	info@recro-net.hr

Dodatni slajdovi

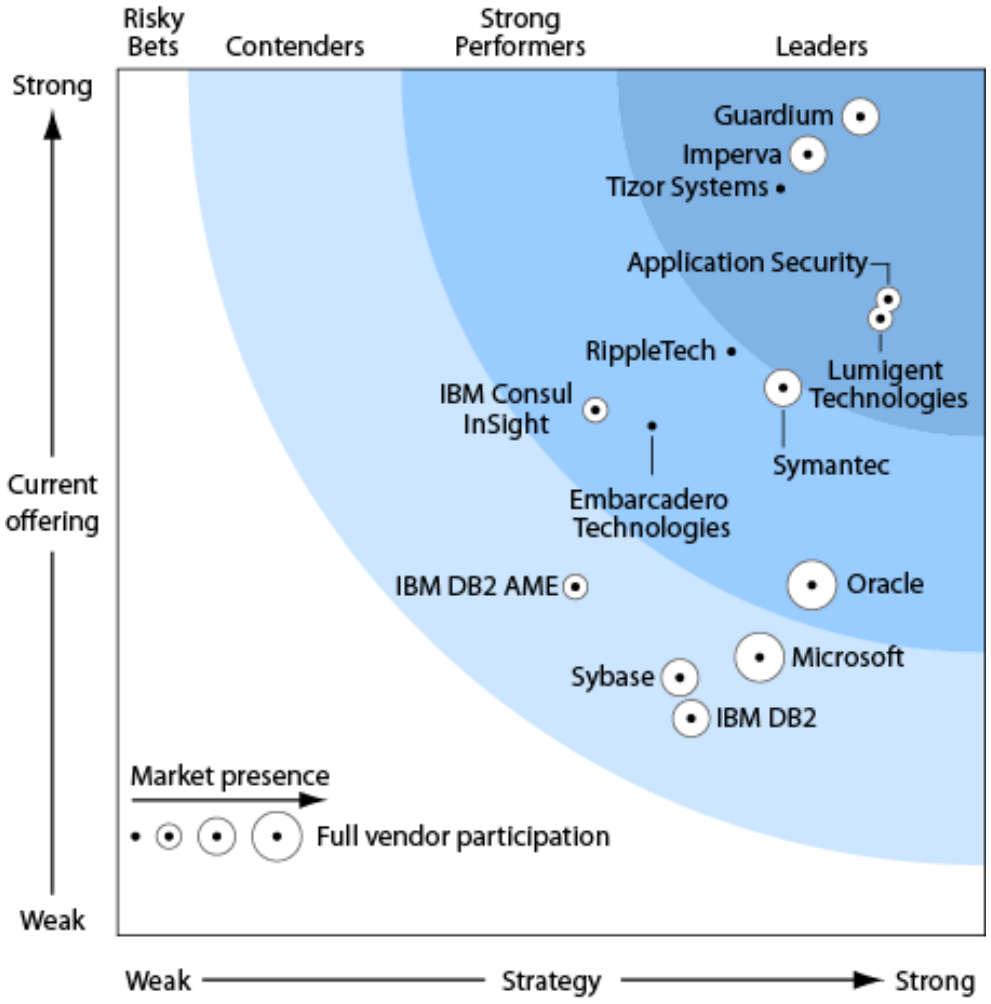
Kako Guardium pomaže kod PCI DSS

PCI Requirement	Guardium PCI Capabilities
2: Do not use vendor defaults for system passwords Configure system parameters to prevent misuse Encrypt non-console admin access	✓ Checks for misconfigured accounts, privileges, etc. ✓ Tracks & audits usage and alerts on misuse ✓ Locks configurations after vulnerabilities remediated ✓ Monitors encrypted traffic (Oracle ASO, SSL, etc.)
3: Protect stored cardholder data	✓ Prevents unauthorized access to sensitive tables ✓ Compensating control for DBMS encryption ✓ Auto-discovers & classifies sensitive data, and identifies movement of CVV/PIN data
6: Maintain secure systems Establish a process to identify newly discovered security vulnerabilities Follow change control procedures for all configuration changes.	✓ Ensures all current patches applied ✓ Provides ongoing updates via subscription service ✓ Monitors & alerts on all configuration changes ✓ Reconciles changes to ticketing systems (Remedy, etc.) ✓ Protects Web applications from attacks (e.g., SQL injection) via anomaly detection
7: Restrict access to cardholder data	✓ Provides granular access controls, including blocking privileged users from unauthorized access to sensitive tables (S-GATE)
8: Assign a unique ID to each person with computer access; enforce password policies; limit repeated access attempts	✓ Alerts on sharing of credentials (incl. at application layer), failed logins, account creation, priv. escalation ✓ Verifies password policies enforced; locks accounts
10: Track & monitor access to cardholder data	✓ Creates secure audit trail about *who, what, when, where, how* of all database access (incl. priv. users) ✓ Automates report distribution & sign-off process

Highest Overall Score for Current Offering, Corporate & Product Strategy

FORRESTER®

- "Dominance in this space."
- "A Leader across the board."
- "Leadership in supporting large heterogeneous environments,… high performance and scalability, simplifying administration …and real-time database protection."
- "Strong road map ahead with more innovation and features."



Source: "The Forrester Wave™: Enterprise Database Auditing and Real-Time Protection, Q4 2007" (October 2007)

Scenariji upotrebe

Slučaj 1: Automatsko pronalaženje baza

U organizaciji s više database servera i brojnim bazama podataka, pronalaženje baza može biti veliki izazov.

Ponekad se baze pojave u produkcijskoj okolini izvan uobičajenih kontrolnih mehanizama. Na primjer, nova baza podataka može biti integralni dio nekog novog aplikacijskog paketa. U starijim instalacijama, neke baze podataka mogu ostati bez nadzora ili su u potpunosti zaboravljene. Moguće je i da DBA kreira novu instancu baze i radi s njom po svojoj volji bez odgovarajućeg nadzora svojih aktivnosti.

Auto discovery funkcionalnost Guardiuma se može iskoristiti za pretraživanje mreže i automatsku prijavu svih otkrivenih baza. Postupak je moguće periodički ponavljati i o rezultatima automatski izraditi izvještaj.

Slučaj 2: Otkrivanje osjetljivih podataka

Međunarodna banka je tokom godina prebrodila brojna spajanja i kupovine manjih banaka.

Nakon svake od tim promjenama, informacijski sustav i baze podataka banke su narasli i danas osjetljive informacije poput broja kreditnih kartica, transakcije, osobne financije se nalaze na više lokacija u više različitih sustava.

Skrbnicima podataka je postalo teško da pronađu i klasificiraju osobne podatke. Banka je shvatila da je teško osigurati podatke i upravljati rizikom kad je osjetljivost pohranjenih podataka nepoznata.

Guardium se može iskoristiti za pronalaženje osjetljivih podataka u bazama podataka bez obzira gdje se fizički nalazili. Pronađeni podaci se mogu iskoristiti za kreiranje objekata koji se kasnije koriste za nadzor aktivnosti nad osjetljivim podacima.

Slučaj 3: Revizija promjena i upotrebe podataka

Velika tvrtka zbog usklađenosti sa zakonskom regulativom mora dokazati da se podaci u bazama koriste na odgovarajući način i mora uvesti revizijski sustav na svoje database servere.

Postoje 3 sustava; produkcijski, zrcalna kopija produkcijskog i testna baza za testiranje aplikacija. Zahtjevi revizora su sljedeći:

1. Osjetljive tablice se moraju nadzirati na razini SQL vrijednosti parametara. Osjetljive tablice su tablice koje uključuju brojeve kreditnih kartica.
2. Potrebno je ignorirati sve SQL upite prema testnoj bazi.
3. Svi ostali podaci se moraju nadzirati, no nije potrebno pratiti SQL vrijednosti parametara.

Guardium nadzire sve pristupe bazi podataka, no bilježe se samo informacije koje su potrebne za reviziju. Na taj način se postiže manje opterećenje sustava i niža cijena cijelog sustava.

Slučaj 4: Onemogučavanje pristupa osjetljivim podacima

Trgovačka tvrtka ima pohranjene osjetljive podatke o on-line narudžbama kupaca koje želi zaštiti.

Posebno se žele zaštiti podaci o kreditnim karticama kupaca i podaci o njihovim narudžbama. Tablica KUPCI sadrži podatke o kreditnim karticama i potrebno ju je zaštititi od neuobičajenih upita poput SELECT BROJ_KREDITNE_KARTICE, IME_KUPCA FROM KUPCI.

Također zbog zaštite privatnosti tvrtka ne želi da se otkriju podaci o transakcijama iz tablice NARUDZBE.

Guardium agent se može iskoristiti kao firewall koji nadzire aktivnosti nad bazom podataka i prekida zabranjene aktivnosti.

Slučaj 5: Nadzor neuobičajenog prometa (korelacija alarma)

Telekom operater održava baze podataka s osobnim informacijama poput ime i prezime, broj telefona, adrese, broja kreditne kartice i drugih osobnih podataka. Operater želi zaštiti navedene baze podataka od zloupotrebe legitimnih korisnika i vanjskih napadača.

Osjetljivi osobni podaci se nalaze u jednoj tabeli i operater želi da se može detektirati ako neko u kratkom vremenu pristupa velikoj količini zapisa iz te tabele. To može značiti da netko pokušava ukrasti osobne podatke.

Guardium može detektirati neuobičajene aktivnosti nad bazom podataka. Pristup podacima u bazi uobičajeno prati određeni obrazac ponašanja gdje se određena količina podataka tipično povlači u nekoj jedinici vremena. Guardium je moguće iskoristiti da detektira odstupanje od uobičajenog obrasca ponašanja.

Slučaj 6: Revizija promjena konfiguracija

Državna agencija trenutno nadzire sve SQL upite prema svojim bazama podataka. Zadovoljni su kako to radi , no svjesni su da je moguće napraviti neke promjene na serverima baza podataka bez izdavanja SQL naredbi. To uključuje promjene konfiguracijskih datoteka servera i konfiguracijskih parametara baze podataka.

Interna revizija zahtjeva da se prate sve promjene konfiguracija. Posebno ih interesira da se prati:

1. Linux host file /etc/hosts
2. Konfiguracijski parametar baze kojem se pristupa naredbom “db2 get dbmcfg”
3. Konfiguracijski parametar baze NARUDZBE kojem se pristupa naredbom “db2 get db cfg for orders”

Guardium može pratiti promjene konfiguracija baza podataka i druge konfiguracijske parametre.

Slučaj 7: Procjena ranjivosti baza podataka

Trgovačka tvrtka želi provjeru sigurnosti svojih baza podataka. Tvrtka je investirala u mrežnu sigurnost, operacijske sustave, antivirusnu zaštitu, antispam sustav kako bi zaštitila osjetljive podatke u svojim bazama podataka. Ipak, tvrtka je svjesna da to vjerojatno nije dovoljno i da su možda njene baze podataka ranjive.

Strukovna regulativa traži periodičku provjeru ranjivosti cijele infrastrukture baza podataka. Provjera mora pronaći nedostatke poput: nepostojeće zakrpe, pogrešno konfigurirana prava pristupa, inicijalni korisnički računi, slabe zaporke, dijeljenje administrativnih prava,učestale prijave administratora i druge rizike.

Guardium raspolaže s opcionalnim modulom za provjeru ranjivosti baza podataka. Izvještaj provjere pokazuje trenutnu razinu rizika. Moguće je automatski uspoređivati rezultate uzastopnih provjera ranjivosti.

Slučaj 8: Usklađivanje upravljanja promjenama

Banka ima uveden sustav za upravljanje promjenama IT sustava. Svaka promjena mora biti najavljena, dokumentirana i odobrena. Interna revizija provjerava da su promjene baza podataka u skladu sa sustavom za upravljanje promjenama.

Banka želi smanjiti cijenu provjere usklađenosti stanja u sustavu za upravljanje promjenama sa stvarnim stanjem. Istovremeno, banka želi poboljšati kvalitetu provjere i osigurati da ni jedna promjena nije provedena izvan odgovarajuće procedure za upravljanje promjenama.

Guardium omogućava bilježenje DDL naredbi i usklađivanje naredbi sa zapisima u sustavu za upravljanje promjenama. Proces revizije je također moguće automatizirati.

Slučaj 9: Automatizacija procesa revizije promjena

Banka traži automatizaciju sljedećeg procesa revizije:

1. Tjedno se izrađuje izvještaj koji sadrži DDL naredbe izvršene na bazi podataka. Izvještaj sadrži broj zahtjeva za svaku promjenu napravljenu na bazi podataka. Svaka promjena koja ne sadrži broj zahtjeva se posebno ističe u izvještaju.
2. Izvještaj se šalje internom revizoru koji odobrava izvještaj. Nakon odobravanja izvještaj se šalje voditelju službe na pregled eventualnih komentara revizora.

Guardium omogućava automatizaciju procesa revizije. Moguće je automatizirati izradu izvještaja potrebnih za reviziju kao i proces odobravanja i bilježenja primjedbi revizora.