Dbaj o bezpieczeństwo danych firmy

IBM InfoSphere Guardium

Artur Wroński
IBM Information Management
artur.wronski@pl.ibm.com

Zabezpieczanie baz danych

By uniknąć wewnętrznych zagrożeń:

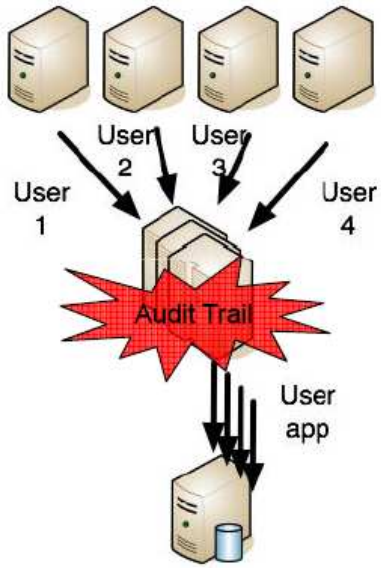
- Nieuprawnione modyfikacje danych
- Wyciek danych poza firmę

By uniknąć zewnętrznych zagrożeń:

- Kradzież danych

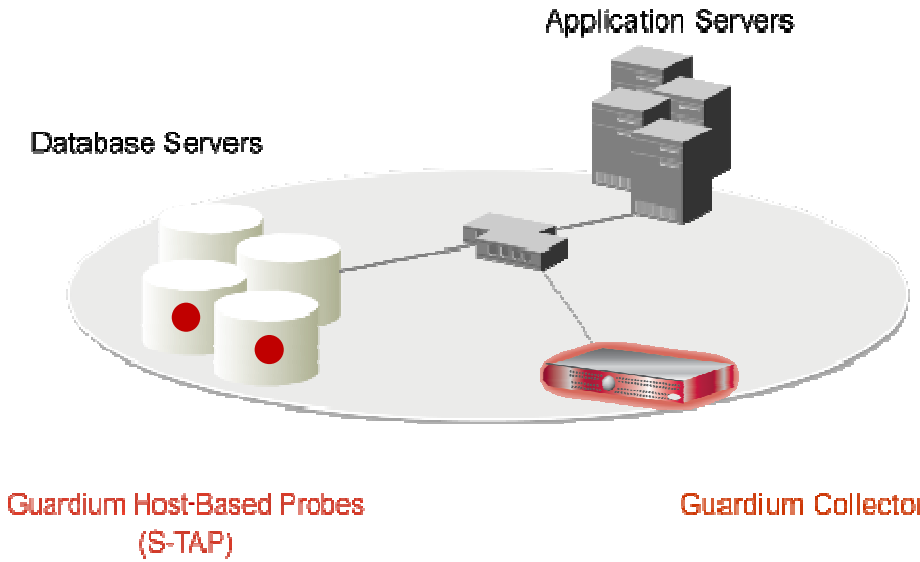
By zapewnić zgodność z regulacjami

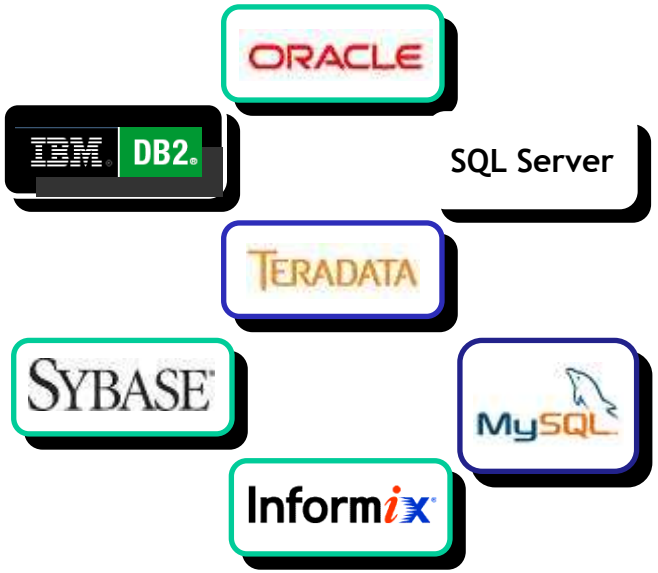
Natywny audyt bazy danych?



- Bardzo niekorzystny wpływ na wydajność bazy !
- Brak granularności w zbieraniu informacji i raportowaniu
- Utrata kontekstu użytkownika przy wykorzystaniu serwerów aplikacyjnych
- Brak czystego podziału obowiązków: administracja bazą - zarządzanie bezpieczeństwem
- Trudny w użyciu, bo każda baza ma swój, zupełnie różny mechanizm audytu

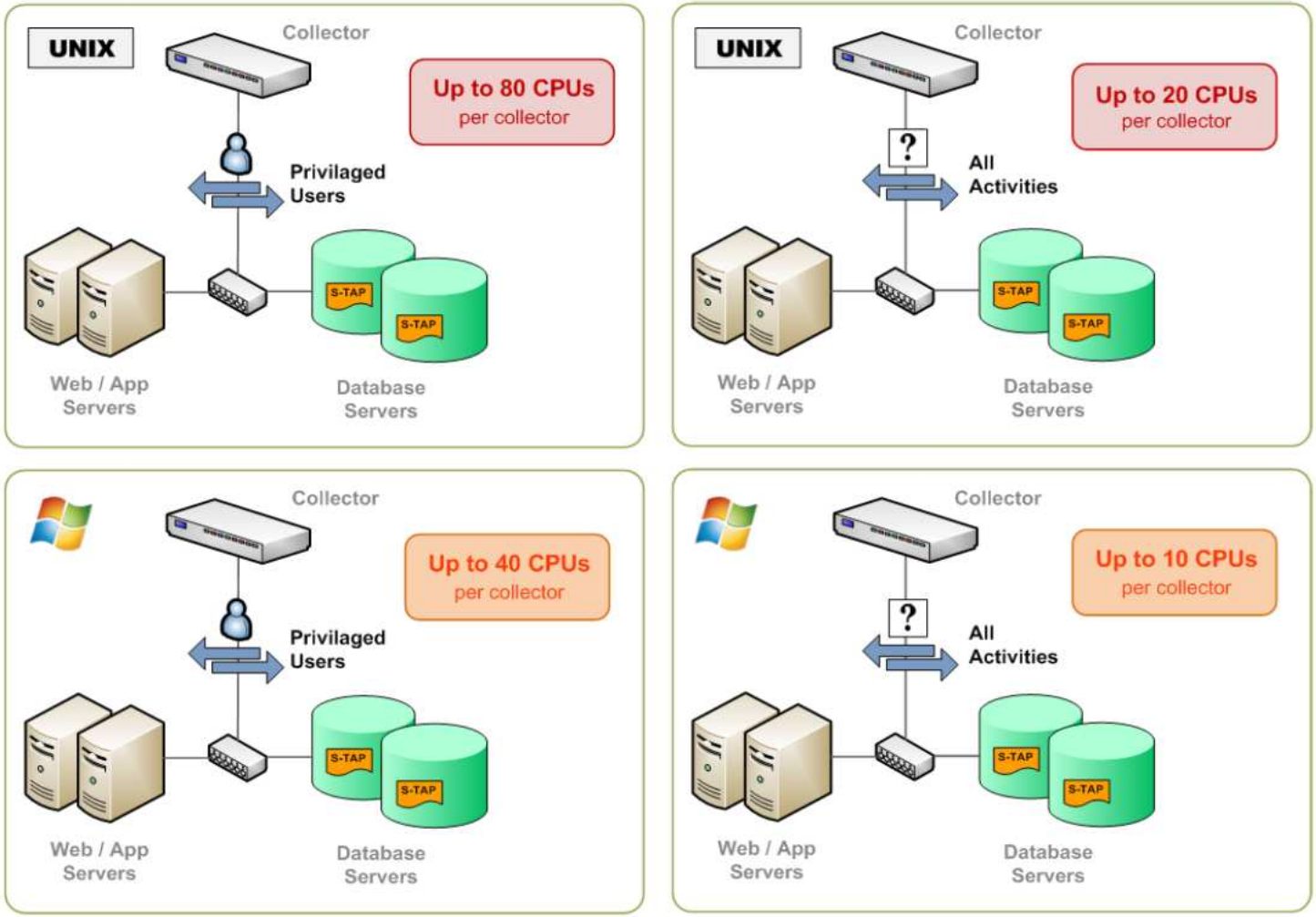
Guardium - architektura



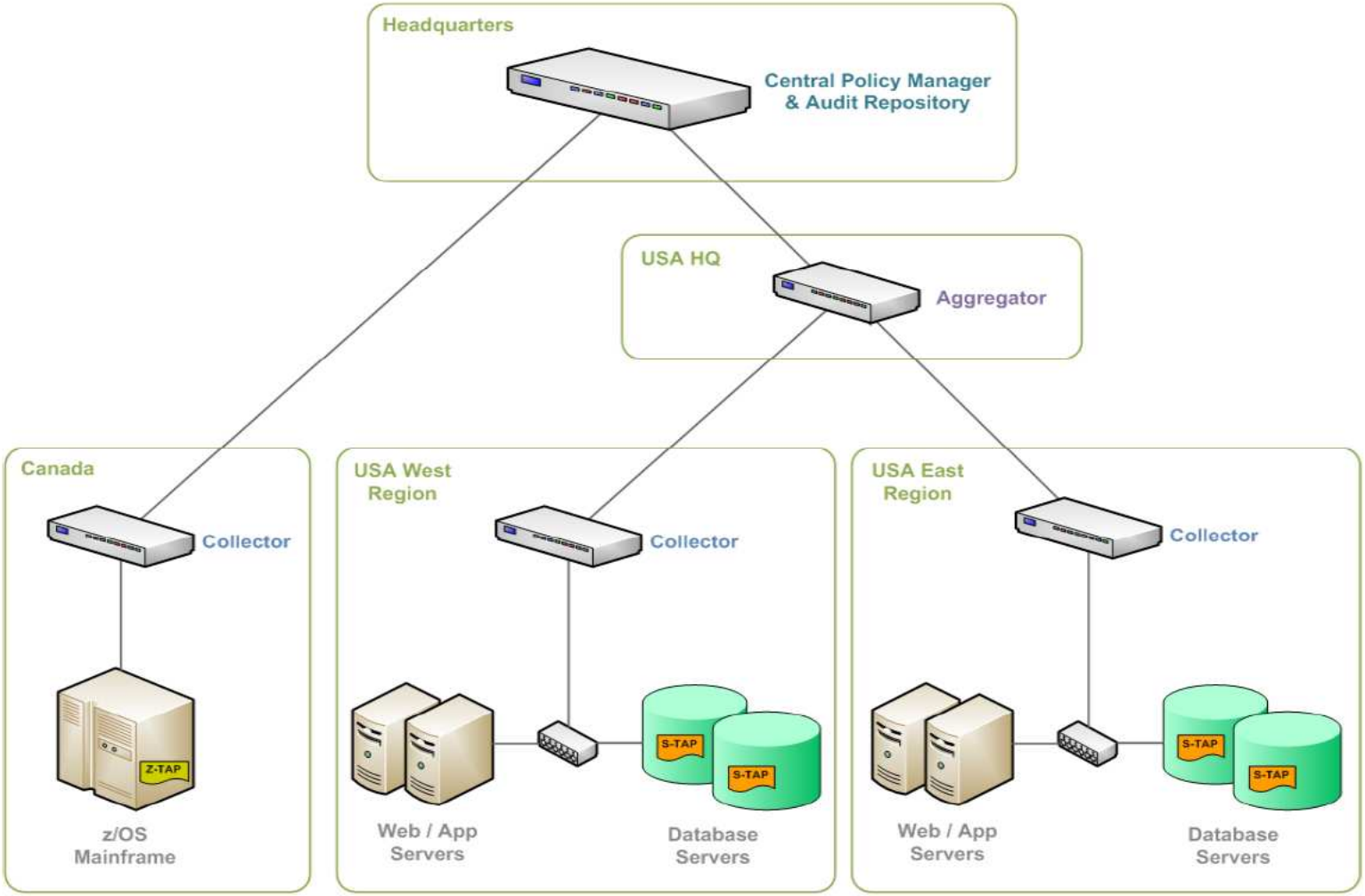


- Nieinwazyjna architektura
  - Na zewnątrz bazy danych
  - Minimalny wpływ na wydajność (2-3%)
  - Nie wymaga żadnych zmian w DBMS lub aplikacji
- Obsługuje wiele różnych baz danych
- 100% widoczność włączając lokalny dostęp przez DBA
- Wymusza rozdzielność uprawnień
- Nie wykorzystuje logów baz danych podatnych na usunięcie, zmiany
- Szczegółowe, działające w czasie rzeczywistym polityki i zestawy reguł audytu
  - *Kto, co, kiedy, jak*
- Zautomatyzowane raportowanie zgodne z wymaganiami regulacji prawnych i audytów (SOX, PCI, NIST, etc.)

Guardium - wymiarowanie



Guardium – modułowa architektura



Przegląd funkcjonalności

Demo !