GDPR - Esperienze concrete e casi di successo

Ancona, 23 Novembre 2017

Fabbiano Ettore – Client Delivery Manager

Vantea Smart
"Chi siamo"

Vantea Smart: System Integrator e Gold Partner Oracle

Ambito Security

- *consulenza progettuale*
- *sicurezza logica applicativa*
- *vulnerability assessment*
- *penetration test*
- *sicurezza perimetrale*

Ambito GDPR

- *Consulenza: privacy, normative, organizzazione e processi*
- *Progetti: sicurezza dei database e dei dati, strutturati e non strutturati*

GDPR

2 casi concreti (Data Security) di clienti in ambito bancario

Caso 1

"Contesto, obiettivi, fasi"

Il contesto

- *30 database*
- *200 utenti*
- *300 applicazioni*
- *>15 amministratori di sistema*

Gli obiettivi

- *Semplificazione operativa*
- *Protezione del dato*
- *Gestione utenze privilegiate sui DB*
- *Segregation of Duties*
- *Monitoraggio e reporting*

Fasi

- *Assessment*
- *Implementazione*
- *Step successivi in Roadmap*

Fase di Assessment

"GDPR – Data Security"

Discovery & Classification

Oracle Application Data Modeling

- Discovery di tabelle e colonne contenenti «Dati Personali»
- Classificazione dei dati personali individuati

Security Assessment

Oracle Security Assessment Tool

- Discovery issues su configurazioni standard lasciate attive
- Discovery di «security configuration errors»
- Discovery accessi privilegiati

Article 35 - *The controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.*

VANTEA SMART

Implementazione

"GDPR – Data Security"

Controllo degli accessi privilegiati e regole di SoD

- Definizione di "Realm" (insieme di tabelle, viste, colonne, etc…) che prevedono accesso ad-hoc degli utenti privilegiati: i DBA
- Definizione utenze Nominali
- Definizione utenze Applicative
- Definizione di regole e policy di SoD

Oracle Database Vault

Funzioni e i privilegi che prima erano propri di un **unico "super-user"** sono stati suddivisi **tra diversi ruoli** con determinati privilegi

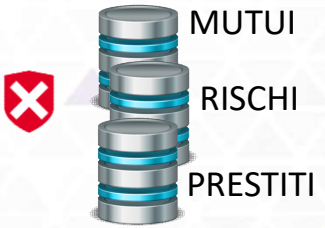
Article 29 - *… Processor and any person … who has access to personal data, shall not process those data except on instructions from the controller..*

Implementazione

"GDPR – Data Security"

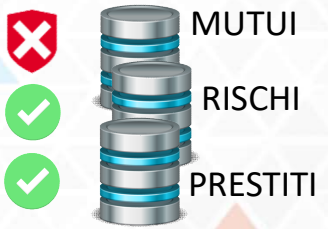
Il DBA opera correttamente e non può vedere i dati applicativi

select * from MUTUI.process
select * from RISCHI.tb_fam_family
select * from PRESTITI.phmon



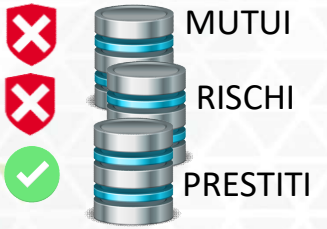
User Nominale A appartiene ai realm RISCHI e PRESTITI

select * from MUTUI.process
select * from RISCHI.tb_fam_family
select * from PRESTITI.phmon



User Nominale B appartiene al realm PRESTITI

select * from MUTUI.process
select * from RISCHI.tb_fam_family
select * from PRESTITI.phmon



Implementazione

"GDPR – Data Security"

Centralizzazione e governance delle utenze DB

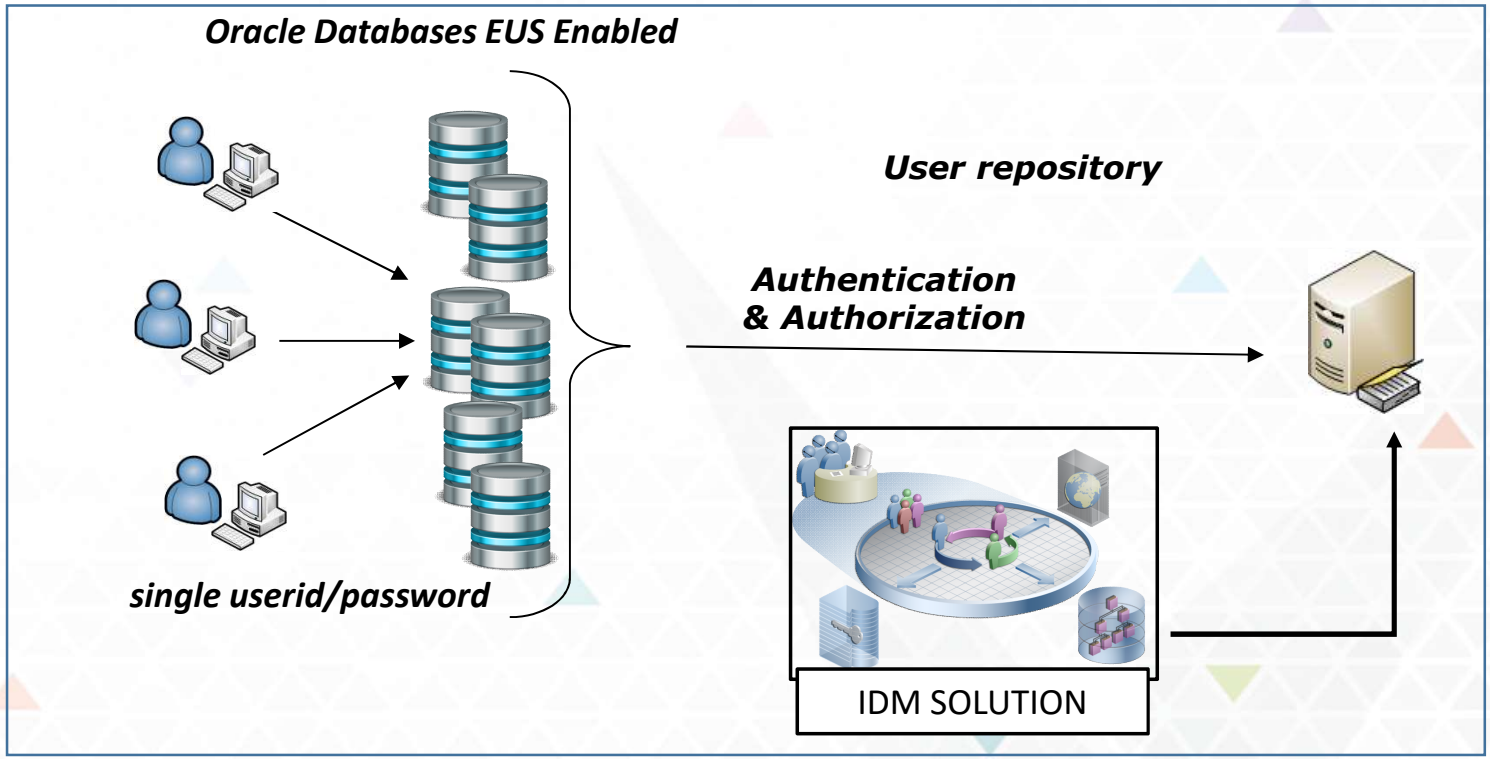
- Definizione e gestione delle utenze DB in un unico repository (LDAP)
- Gestione e assegnazione dei privilegi mediante un'unica console
- Password policy valide per l'accesso a tutti i DB
- Governance delle utenze mediante una soluzione di Identity Management
- Unica coppia di credenziali per ogni utente per l'accesso ai DB

Oracle EUS

Implementazione

"GDPR – Data Security"

Governance e controllo centralizzato delle utenze DB



Caso 2

"Contesto, obiettivi, fasi"

Il contesto

- *ORACLE: 94 Produzione + 87 Non Produzione*
- *DB2: 33 Produzione + 37 Non Produzione*
- *MSSQL: 31 Produzione + 11 Non Produzione*
- *TOT: 158 Produzione + 135 Non Produzione*

Fasi

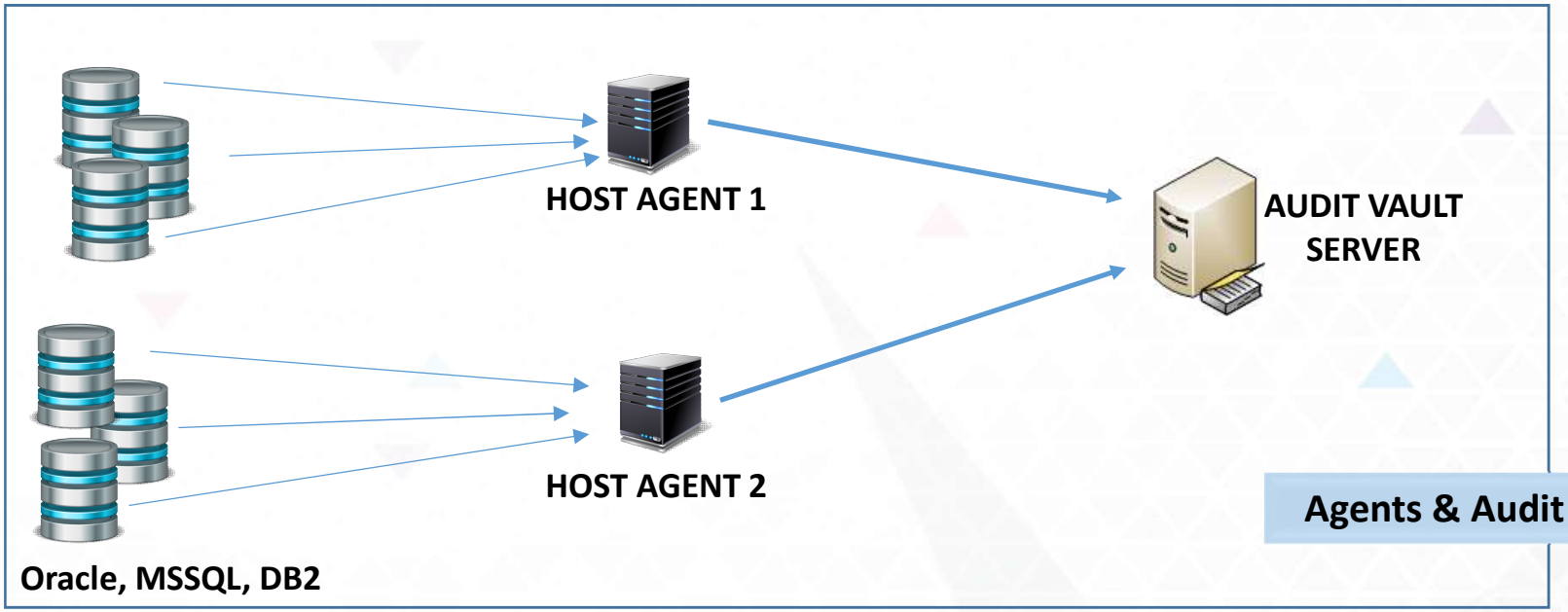
- *Assessment*
- *Implementazione*
- *Step successivi in Roadmap*

Gli obiettivi

- *Tracciare i Log-in e log-out delle utenze Amministratori di Sistema*
- *Tracciare le operazioni considerate "amministrative"*
- *Conservare i dati raccolti*
- *Predisposizione console per monitoraggio e consultazione dati (reporting)*
- *Definizione di alert per eventi critici in funzione di regole e policy pre-definite*

Implementazione: step 1

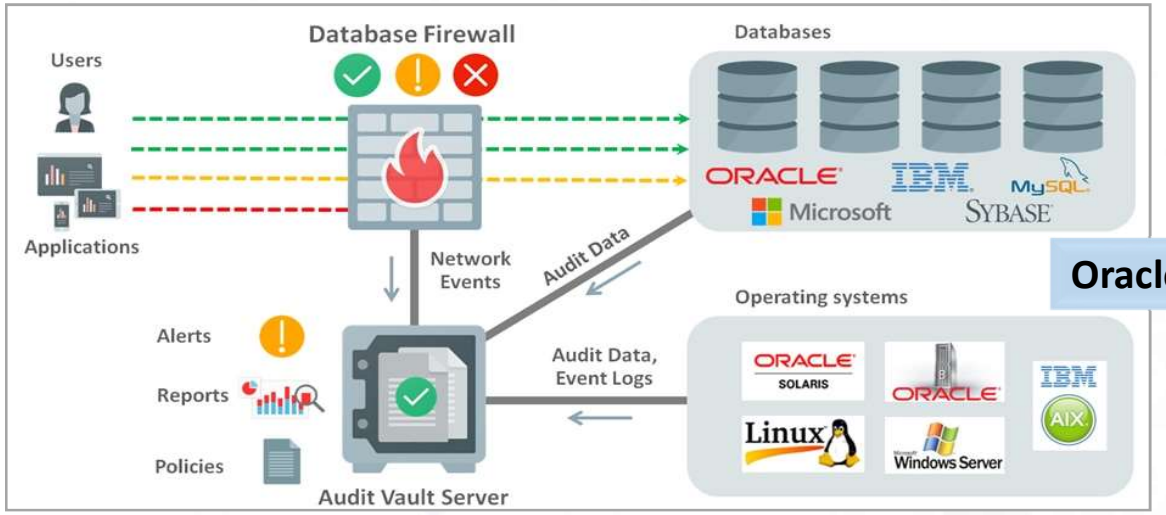
"Contesto, obiettivi, fasi"



- Invio degli audit trace verso i remote agents
- Invio degli audit trace verso l'audit server
- Consultazione audit e report attraverso la console

Implementazione: step 2

"Contesto, obiettivi, fasi"



Oracle DB Firewall & Audit Vault

- Monitoraggio e blocco del traffico SQL non autorizzato o malevolo prima che raggiunga il DB
- Monitoraggio degli accessi ai database
- Gestione di "white" o "black" list per utenti e applicazioni
- Report di Audit e Compliance personalizzati

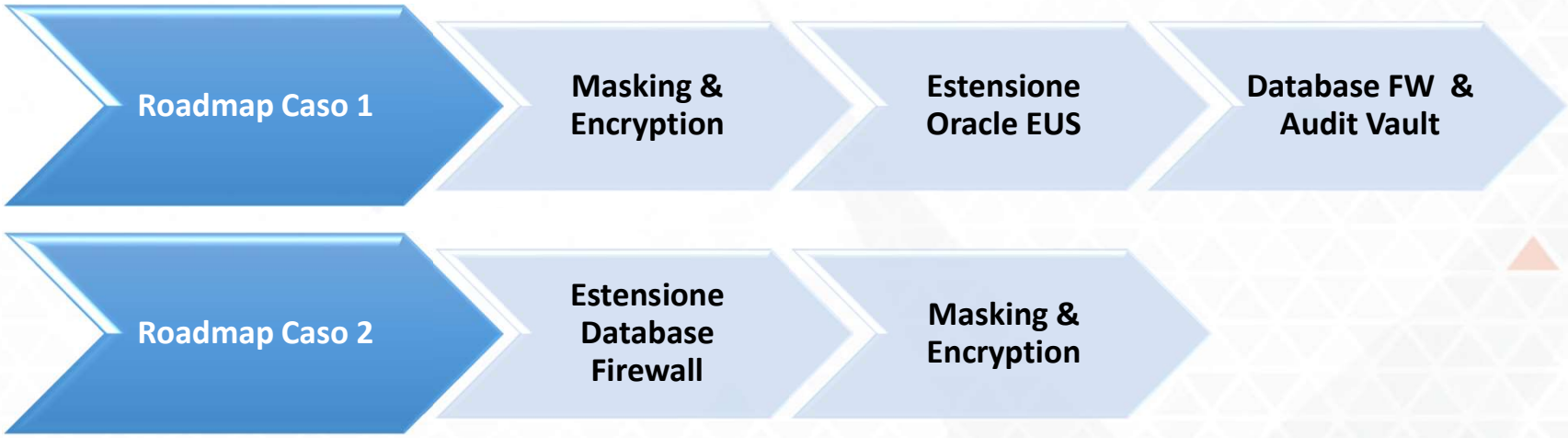
Article 30 - *Each controller ... shall maintain a record of processing activities under its responsibility.*

Article 33 - *"In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority ..."*

Fasi in roadmap

"GDPR – Data Security"

Roadmap condivise con i rispettivi clienti per i prossimi step riguardo l'ambito Data Security GDPR



GDPR Data Security

Assessment & Discovery

- Dati strutturati e non strutturati
- Classificazione dei dati
- Identificazione dati personali

Oracle Application Data Modeling
Oracle Database Vault
Oracle Database Security Assessment Tool

Prevention

- Encryption dei dati personali/sensibili
- Mascheramento dei dati sensibili su ambienti di non-produzione
- Controllo accessi privilegiati (DBA)
- Definizione di regole e policy di SoD

Data Encryption
Data Masking, Redaction, Subsetting
Oracle Database Vault

Monitoring/Detection

- Centralizzazione e memorizzazione delle operazioni eseguite sui dati
- Analisi e reporting sulle operazioni eseguite sui dati
- Monitoraggio del traffico verso i DB
- Rilevazione azioni anomale
- Blocco di eventuali azioni rilevate come anomale

Oracle Audit Vault
Oracle Database Firewall

Q&A

Grazie per l'attenzione

Oracle & Vantea Smart

Ettore Fabbiano