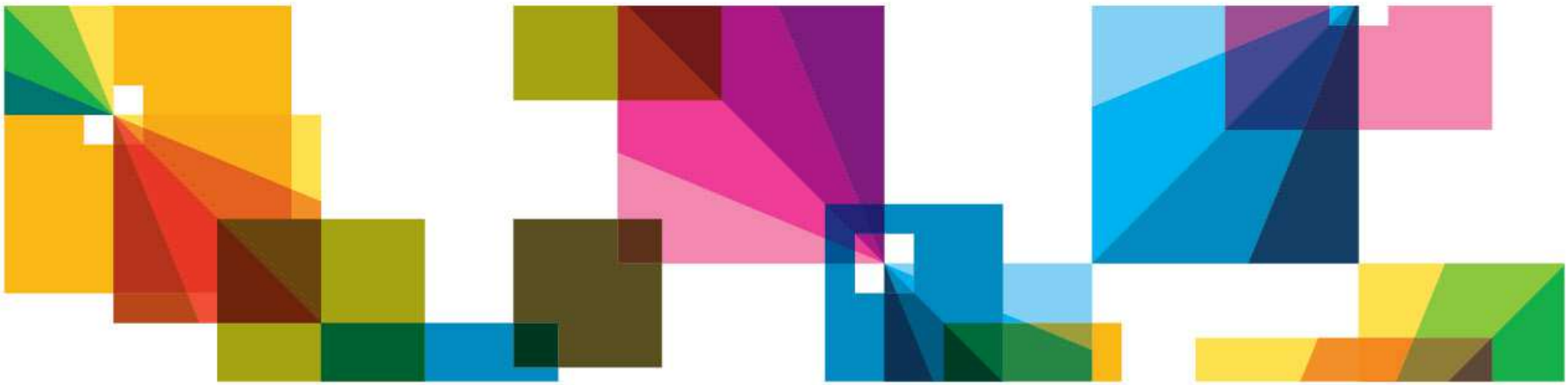
Smarter Analytics Live

IBM

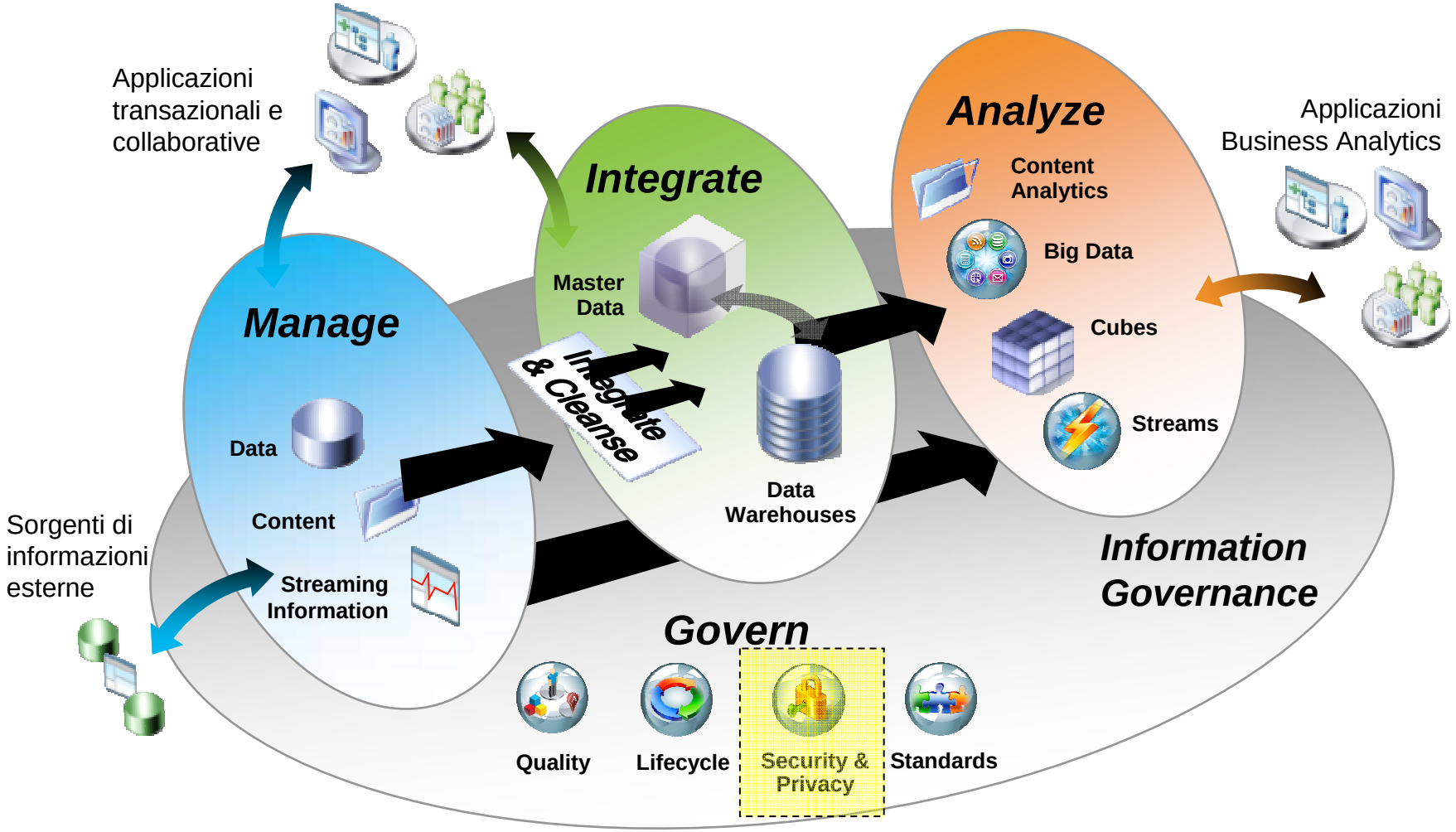
Il Sole 24 ORE

Sergio Mucciarelli

Information Governance: la chiave per informazioni sicure e conformi a leggi e regolamenti



L’importanza dell’information governance si espande attraverso l’intera catena di fornitura delle informazioni

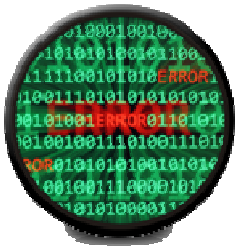


La sicurezza dei Database

Come quantificare il rischio?

Hackers obtained personal information on 70 million subscribers.

April 2011: *Malicious outsiders stole name, address (city, state, zip), country, email address, birth date, PlayStation Network/Qriocity password and login, and handle/PSN online ID, and possibly credit card numbers from 70 million Sony PlayStation users.*



SQL injection is fast becoming one of the biggest and most high profile web security threats.

April 2011*: A mass SQL injection attack that initially compromised 28,000 websites shows no sign of slowing down. Known as LizaMoon, this malicious code is after anything stored in a database.*

Unprotected test data sent to and used by test/development teams as well as third-party consultants.

February 2009: *An FAA server used for application development & testing was breached, exposing the personally identifiable information of 45,000+ employees.*

Hundreds of thousands of secret reports regarding US wars in Iraq and Afghanistan published on WikiLeaks.

December 2010: *A private in the US military, downloaded top secret military documents and passed them to journalist for publication. This puts US national security at risk as well as the lives of those named in reports.*

I Business Drivers chiave sulla sicurezza dei database

Monitoring continuo sui dati sensibili:

1. Prevenire il furto di dati

- Cybercriminals
- Proteggere dati Cliente e segreti corporate (IP)

2. Supportare la data governance

- Prevenire cambiamenti non autorizzati sui dati sensibili da parte di utenti privilegiati

3. Ridurre i costi di audit

- Automatizzare, controlli in continuità
- Processi semplificati

Policy sulla Sicurezza: identificazione ed azioni

Identification: who, what, when, where, and how of each transaction

- Who: database user, application user, OS user
- What: database, field name, sensitive object
- When: time period, working hours, after hours
- Where: client IP, server IP
- How: access, data extrusion, SQL/login exception



Action: enforcement of rule

- Logging
- Alerting
- Termination

Identification + Action = Security Rule → **Fine-Grained Security Policy**

Le informazioni chiave dei report di sicurezza Guardium

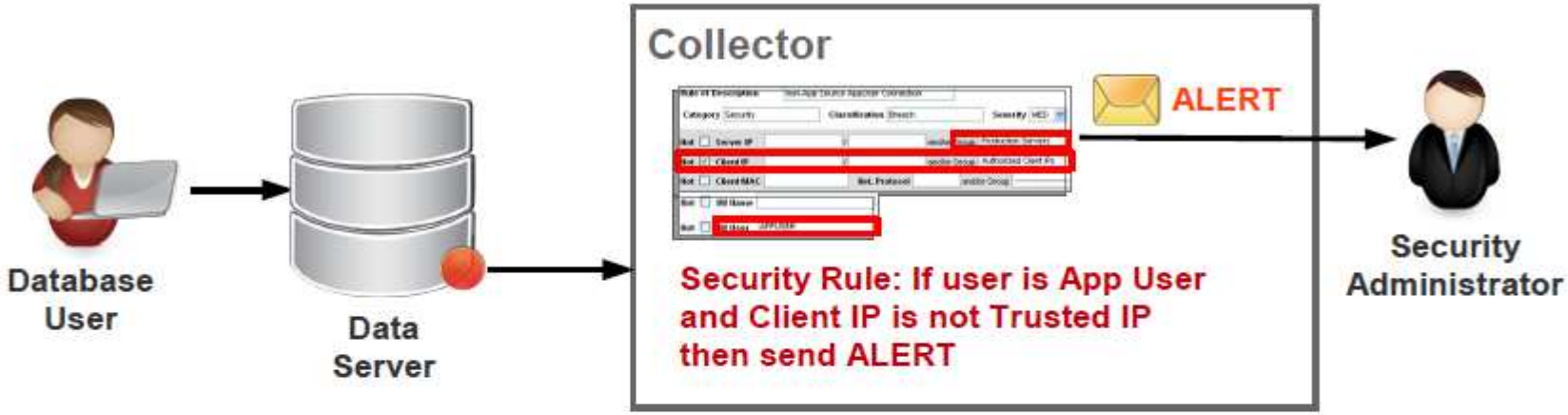
All SQL Constructs

Start Date: 2010-11-08 16:10:50 End Date: 2010-11-08 19:10:50
Aliases: ON DB_Username: LIKE GUARD

Timestamp	Server IP	Server Type	Database Name	DB User Name	Sql	Total access
2010-11-08 19:09:55.0	10.10.9.28	ORACLE	Customer	GUARD	BEGIN DBMS_APPLICATION_INFO.SET_MODULE(:?,NULL); END;	2
2010-11-08 19:09:55.0	10.10.9.28	ORACLE	Customer	GUARD	BEGIN DBMS_OUTPUT.DISABLE; END;	1
2010-11-08 19:09:55.0	10.10.9.28	ORACLE	Customer	GUARD	DELETE FROM CUSTOMERS WHERE CUST_ID=?	3
2010-11-08 19:09:55.0	10.10.9.28	ORACLE	Customer	GUARD	DELETE FROM DETAILS WHERE ITEM_ID=?	9
2010-11-08 19:09:55.0	10.10.9.28	ORACLE	Customer	GUARD	DELETE FROM ITEMS WHERE ITEM_ID=?	9
2010-11-08 19:09:55.0	10.10.9.28	ORACLE	Customer	GUARD	INSERT INTO CUSTOMERS VALUES(?, ?, ?, NULL, NULL, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, NULL, NULL)	1
2010-11-08 19:09:55.0	10.10.9.28	ORACLE	Customer	GUARD	INSERT INTO ITEMS VALUES(?, ?, ?, ?, ?, ?)	9
2010-11-08 19:09:55.0	10.10.9.28	ORACLE	Customer	GUARD	SELECT * FROM CUSTOMERS WHERE CUST_ID=?	20
2010-11-08 19:09:55.0	10.10.9.28	ORACLE	Customer	GUARD	SELECT * FROM ITEMS WHERE ITEM_ID=?	12
2010-11-08 19:09:55.0	10.10.9.28	ORACLE	Customer	GUARD	SELECT ATTRIBUTE,SCOPE,NUMERIC_VALUE,CHAR_VALUE,DATE_VALUE FROM SYSTEM.PRODUCT_PRIVS WHERE (UPPER(?) LIKE UPPER(PRODUCT)) AND (UPPER(USER) LIKE USERID)	1
2010-11-08 19:09:55.0	10.10.9.28	ORACLE	Customer	GUARD	SELECT CHAR_VALUE FROM SYSTEM.PRODUCT_PRIVS WHERE (UPPER(?) LIKE UPPER(PRODUCT)) AND ((UPPER(USER) LIKE USERID) OR (USERID = ?)) AND (UPPER(ATTRIBUTE) = ?)	1
2010-11-08 19:09:55.0	10.10.9.28	ORACLE	Customer	GUARD	SELECT DECODE(?,?,?,?) FROM DUAL	1
2010-11-08 19:09:55.0	10.10.9.28	ORACLE	Customer	GUARD	select EXTRUSION_RULE from sysDummy	1
2010-11-08 19:09:55.0	10.10.9.28	ORACLE	Customer	GUARD	select KBYTE_COUNT from SESSION_COUNTERS	1
2010-11-08 19:09:55.0	10.10.9.28	ORACLE	Customer	GUARD	SELECT USER FROM DUAL	1
2010-11-08 19:09:55.0	10.10.9.28	ORACLE	Customer	GUARD	UPDATE CUSTOMERS SET CITY=? WHERE CUST_ID=?	6
2010-11-08 19:09:55.0	10.10.9.28	ORACLE	Customer	GUARD	UPDATE ITEMS SET UNIT_PRICE = UNIT_PRICE * ?	2

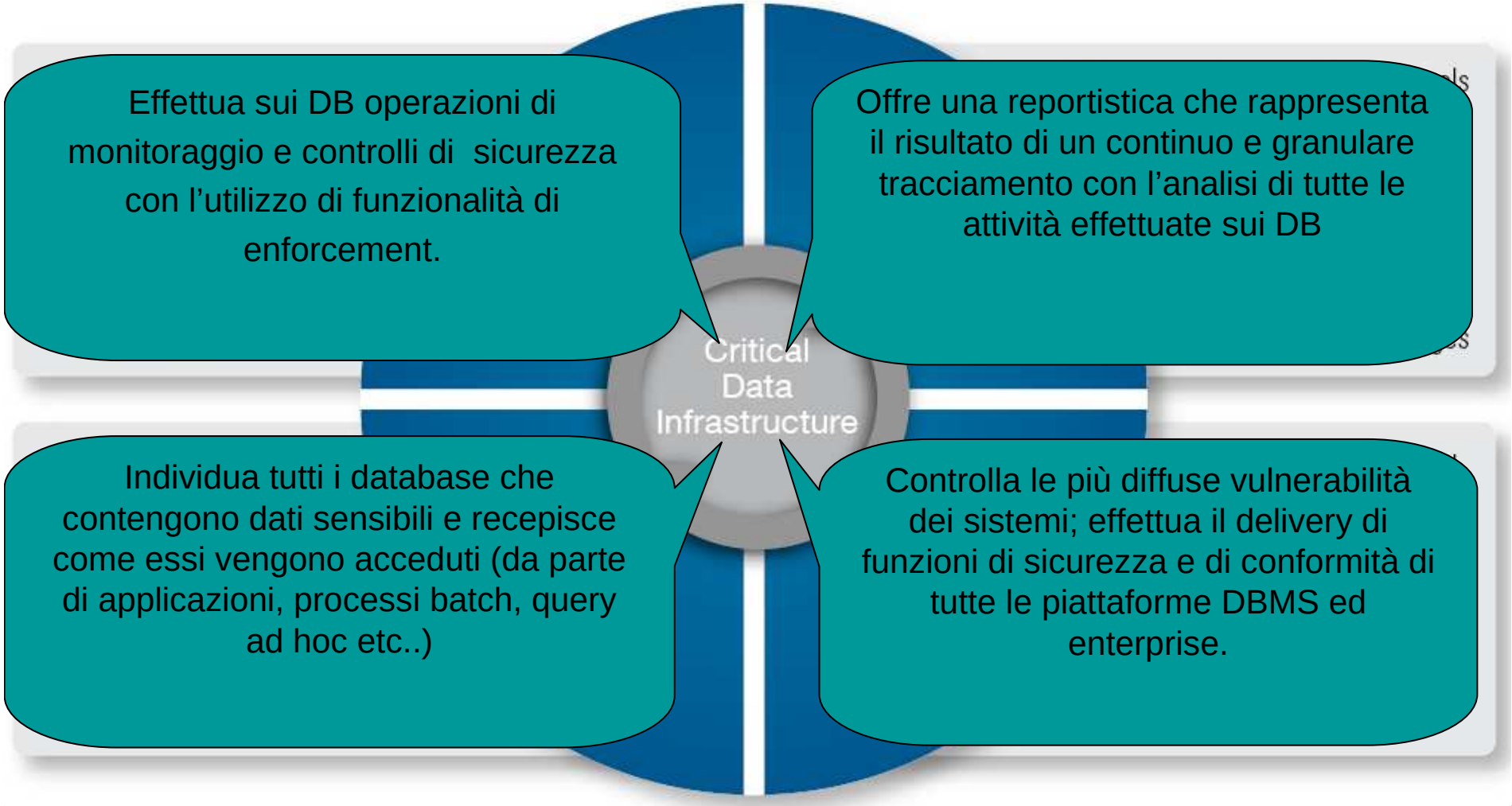
La gestione degli alerts attraverso la soluzione Guardium

Real Time Alert: when a request violates a security rule with alerting action

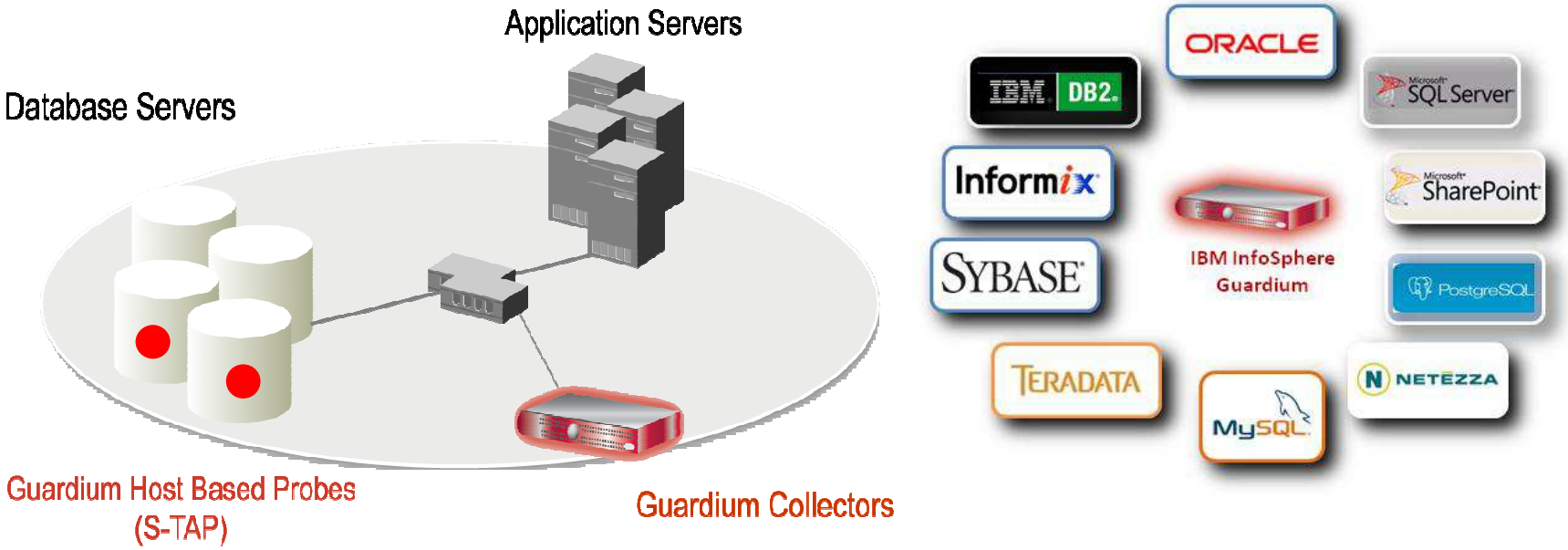


Correlation Alert: when anomaly detected in historic database activity

InfoSphere Guardium : indirizzare tutte le tematiche del ciclo di vita della gestione della sicurezza delle informazioni



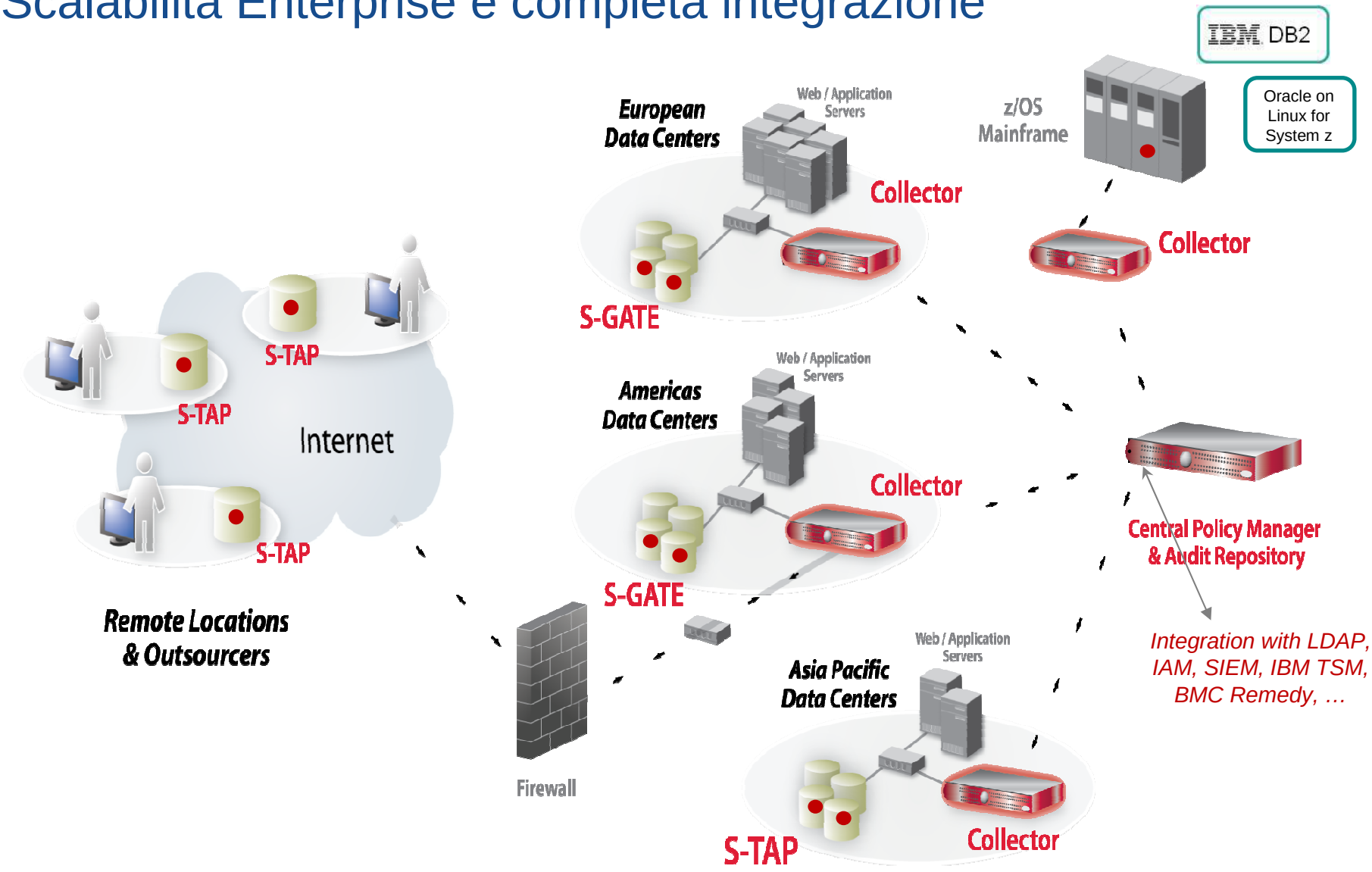
La soluzione architetturale di Guardium



- Architettura non-invasiva
  - Outside database
  - Impatto minimale sulle performance (3 - 5%)
  - No cambiamenti sul DBMS o applicazioni
- Soluzione Cross-DBMS
- 100% visibilità inclusi gli accessi locali dei DBA

- Rinforza la separation of duties
- Non rilascia log residenti su DBMS che possono facilmente essere manomessi
- Auditing granulare, policy in real-time
- *Who, what, when, how*
- Reporting di compliance automatico, sign-offs & escalations (SOX, PCI, NIST, etc.)

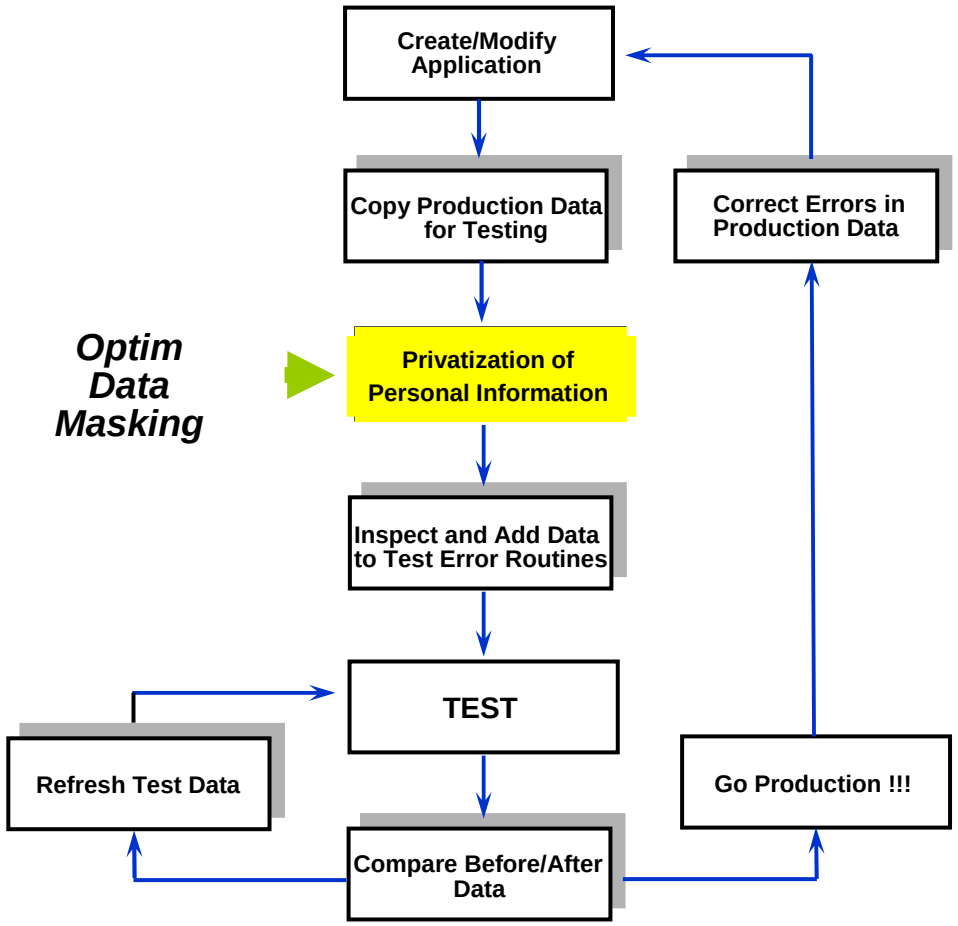
Scalabilità Enterprise e completa integrazione



Soluzioni per il mascheramento dei dati degli ambienti di sviluppo, test e collaudo

Gestione degli ambienti di test e della Data Privacy

- Gestire al meglio i dati negli ambienti di test e di collaudo
  - I dati devono essere rappresentativi delle informazioni reali
  - Devono essere ridotte al minimo le attività di manipolazione dei dati negli ambienti di test e collaudo
  - Devono essere **garantite la sicurezza e la data privacy** delle informazioni rilevanti
- Cosa attendersi da un sistema di archiviazione?
  - Supporto per recuperare efficenza sulle risorse utilizzate
  - Avere la possibilità di gestire subset di dati reali negli ambienti di test e collaudo
  - Adottare **logiche di mascheramento** per quei dati giudicati sensibili e da proteggere



Il mascheramento Optim: garantire l'integrità referenziale

Dati Originali

Tabella Soggetti

Soggetto	Nome	Indirizzo
08054	Alice Bennett	2 Park Blvd
19101	Carl Davis	258 Main
27645	Elliot Flynn	96 Avenue

Tabella Assegni

Soggetto	Importo	Data Assegno
27645	20.000	20 Giugno 2011
27645	15.000	10 Ottobre 2011

Integrità Referenziale Mantenuta

Dati De-Identificati

Tabella Soggetti

Soggetto	Nome	Indirizzo
10000	Auguste Renoir	Mars23
10001	Claude Monet	Venus24
10002	Pablo Picasso	Saturn25

Tabella Assegni

Soggetto	Importo	Data Assegno
10002	20.000	20 Giugno 2011
10002	15.000	10 Ottobre 2011

Propagare i valori delle chiavi primarie in tutte le tabelle correlate mantenendo la consistenza e l'integrità referenziale nei dati mascherati

Sergio Mucciarelli
Information Management
smucciarelli@it.ibm.com
+39.335.1432985