



Monitorización y Auditoría de Bases de Datos InfoSphere Guardium for z

Sonia Márquez Paz
sonia_marquez@es.ibm.com

Guardium[®]
SAFEGUARDING DATABASES™ AN IBM COMPANY

InfoSphere Guardium Introducción

Monitorización continua en tiempo real de todas las actividades de base de datos para:

1. Prevenir fuga de información y brechas

- Proteger frente a ataques internos y externos



2. Garantizar la gobernabilidad del dato

- Evitar accesos no autorizados y cambios a información sensible (por ejemplo, por usuarios privilegiados)

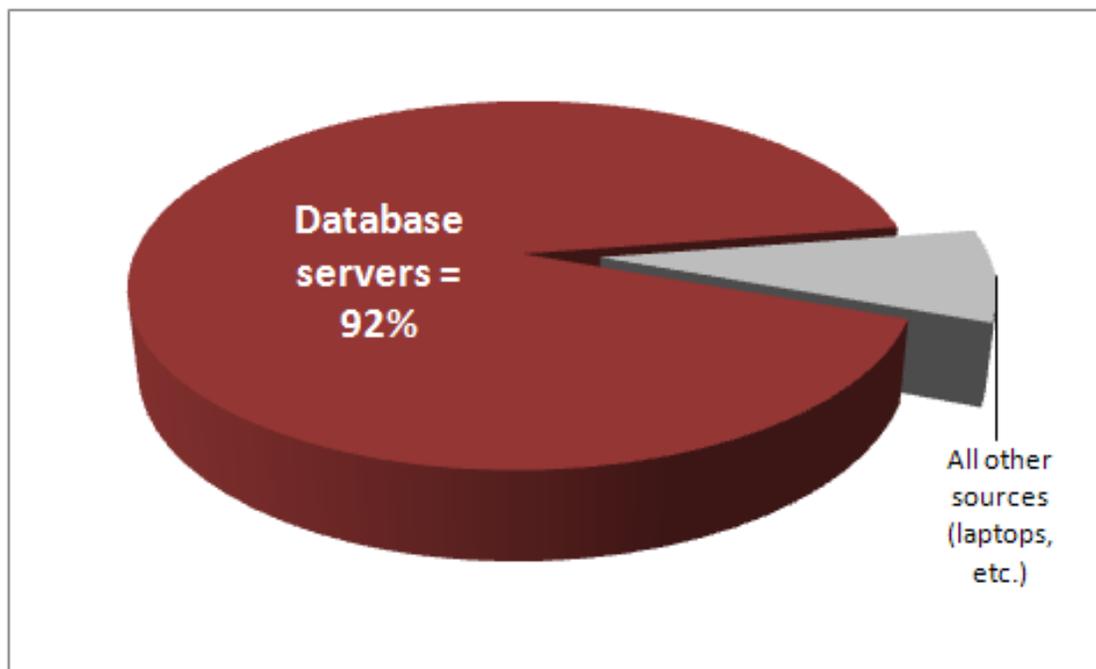


3. Reducir el coste de cumplimiento

- Controles automatizados y centralizados:
 - ✓ Gestores de Bases de Datos (Oracle, DB2, SQL Server, ...)
 - ✓ Enterprise applications (ERP, CRM, HR, analytics, ...)
 - ✓ Normativas y regulaciones (SOX, PCI, LOPD,...)
 - ✓ Unidades de negocio y centros de datos distribuidos
- Mínimo impacto en rendimiento
- Sin cambios en bases de datos o aplicaciones



La mayor parte de los registros comprometidos residen en servidores de bases de datos



http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf

Ataques de SQLInjection: Aumento 134% en 2008

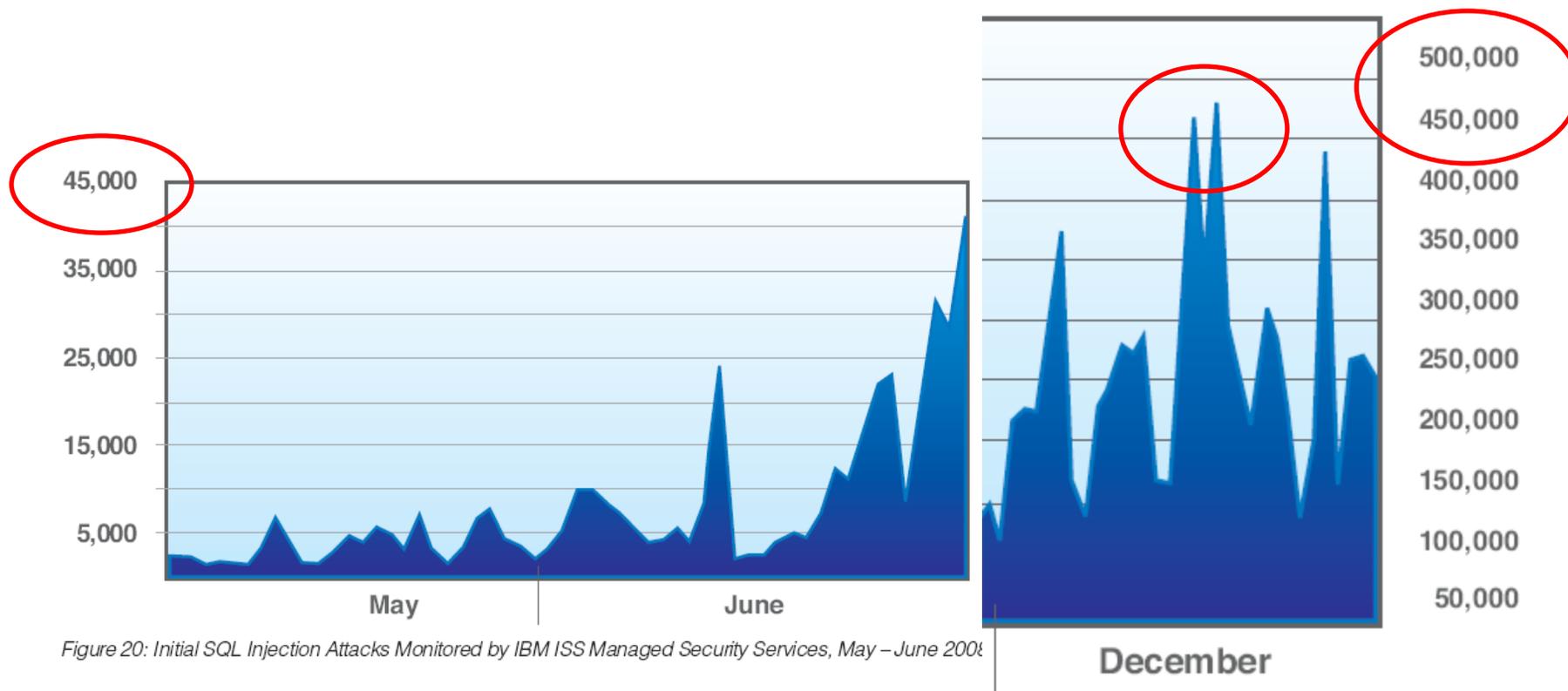


Figure 20: Initial SQL Injection Attacks Monitored by IBM ISS Managed Security Services, May – June 2008

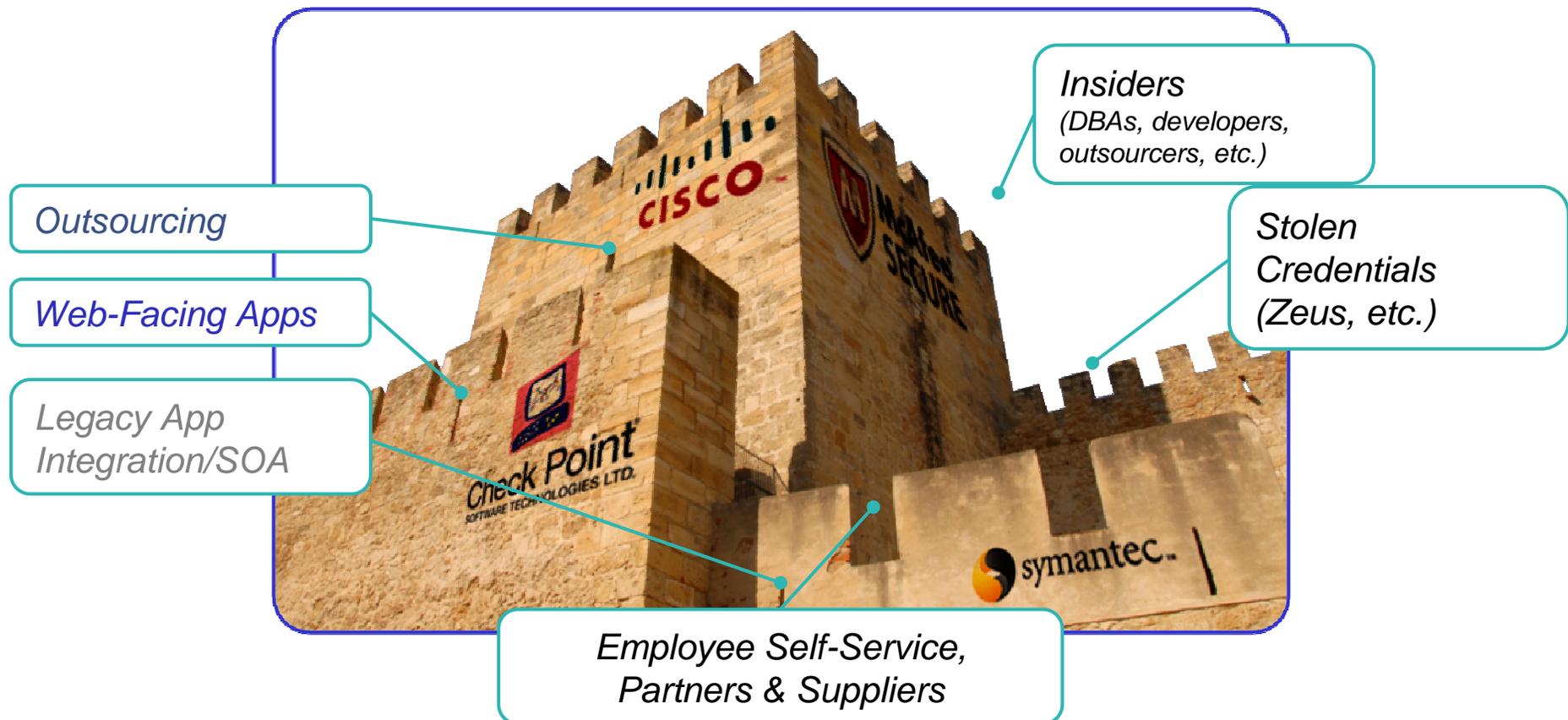
- SQL Injection reemplazó a cross-site scripting como vulnerabilidad #1
- Los nuevos ataques utilizan toolkits automatizados; inyectan malware dentro de las bases de datos
- **"The bad guys are getting in and not being detected." --IBM**

Fuente: IBM Internet Security Systems X-Force® 2008 Trend & Risk Report, Enero 2009

Las defensas perimetrales ya no son suficientes

“A fortress mentality will not work in cyber. We cannot retreat behind a Maginot Line of firewalls.”

- William J. Lynn III,
U.S. Deputy Defense Secretary



Retos habituales: Auditoría DB2 en z/OS



- Presiones de **organismos reguladores** para demostrar que se emplean controles adecuados
 - Especialmente relativos a usuarios privilegiados (DBAs, SYSADMINS, ...)
- La mayor parte de los entornos DB2 en z/OS tienen **auditoría mínima**
 - Requiere un esfuerzo manual, por parte de los DBAs, muy significativo
- El RACF a veces se percibe como un control de seguridad suficiente, aunque el **RACF no**:
 - Evita actualizaciones no autorizadas si el usuario tiene privilegios sobre los datos
 - Previene acceso a datos sensibles que no están en el ámbito de su alcance
 - Proporciona información de detalle de auditoría de qué hizo el usuario mientras accedía a DB2
- No soporta **Separación de Funciones/Roles**, que supone un riesgo potencial de Seguridad
 - Las trazas de DB2 usadas para auditoría son gestionadas por DBAs que están siendo auditados

El Cumplimiento de Regulaciones

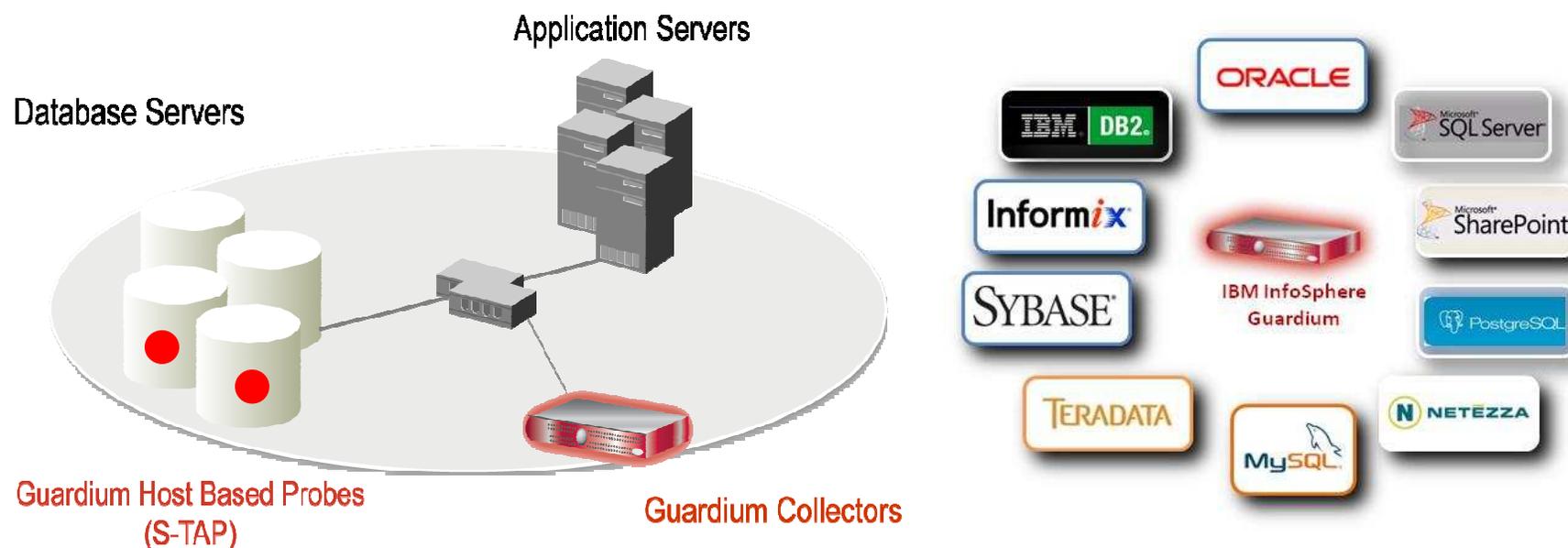
Audit Requirements	COBIT (SOX)	PCI-DSS	ISO 27002	Data Privacy & Protection Laws	NIST SP 800-53 (FISMA)
1. Access to Sensitive Data (Successful/Failed SELECTs)		✓	✓	✓	✓
2. Schema Changes (DDL) (Create/Drop/Alter Tables, etc.)	✓	✓	✓	✓	✓
3. Data Changes (DML) (Insert, Update, Delete)	✓		✓		
4. Security Exceptions (Failed logins, SQL errors, etc.)	✓	✓	✓	✓	✓
5. Accounts, Roles & Permissions (DCL) (GRANT, REVOKE)	✓	✓	✓	✓	✓

DDL = Data Definition Language (aka schema changes)

DML = Data Manipulation Language (data value changes)

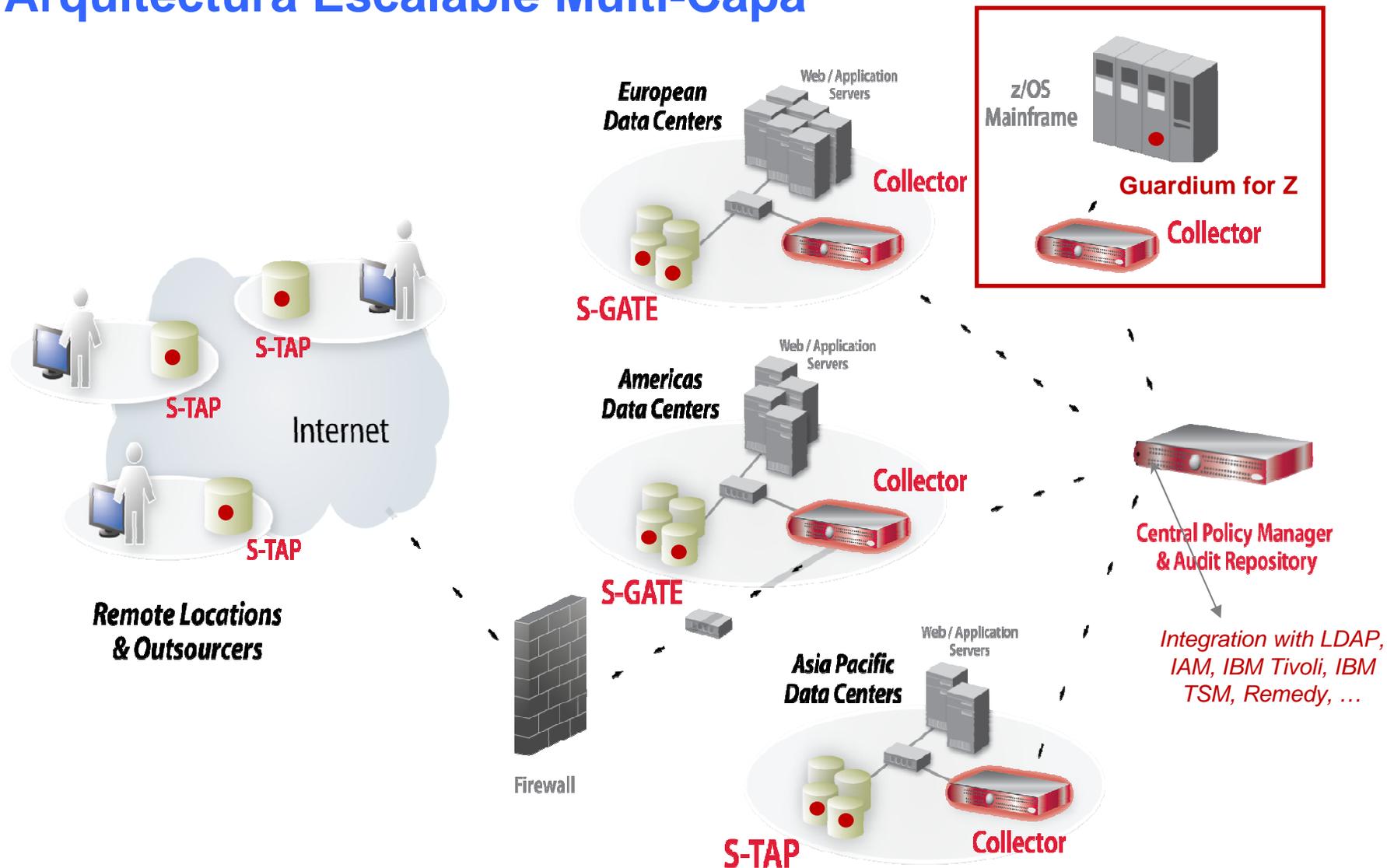
DCL = Data Control Language

Monitorización de Bases de Datos en Tiempo Real



- **Arquitectura no-invasiva**
 - Fuera de la Base de Datos
 - Impacto mínimo en rendimiento (2-3%)
 - Sin cambios al DBMS o aplicativos
- **Solución multi-plataforma**
- **100% visibilidad incluyendo accesos locales de DBAs**
- **Refuerza segregación de funciones**
- **No depende de los logs nativos del DBMS que pueden ser borrados por atacantes o personal interno**
- **Granular, políticas en tiempo real y auditoría**
 - *Quién, dónde, cuándo, cómo*
- **Informes automatizados de cumplimiento, trazabilidad y escalado (SOX, PCI, NIST, etc.)**

Arquitectura Escalable Multi-Capa



Gestión del ciclo de vida completo de la Seguridad en bases de datos y del Compliance con Guardium

Real-time Database Security & Monitoring



Introducción a InfoSphere Guardium 8

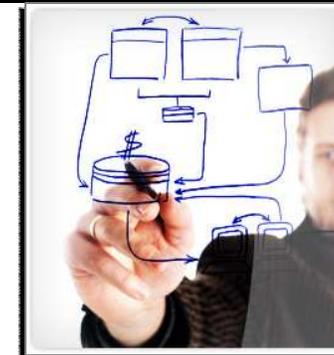
Monitorización de bases de datos más completa para Reducir Riesgos, Simplificar el Cumplimiento de Normativas y Reducir Costes de Auditoría

- El soporte de plataformas más amplio disponible, incluyendo System z
- Monitorización mejorada de SAP para luchar contra el fraude
- Primera solución para monitorizar repositorios SharePoint para acceso a datos sensibles (financieros, diseños, etc.)
- Mitigación de riesgos y seguridad a nivel de datos robusta
 - Desde la monitorización hasta controles de acceso proactivos
 - Bloqueo mejorado: Cuarentena y gestión de Fire-ID
- Reducción del coste y complejidad del cumplimiento
 - Políticas centralizadas y automatizadas para múltiples plataformas y DBMS
 - Automatización avanzada del workflow de compliance



InfoSphere Guardium 8 – Mejoras Adicionales

- **Entitlement reporting**
 - Solución unificada para todos los gestores y plataformas soportadas
- **Mejoras en Vulnerability Assessment**
 - 500 nuevos tests
 - Se añaden tags para el estándar CVE
 - Basado en estándares de la industria CIS Benchmark & DoD STIG
- **Integración con Tivoli Security and Information Management (TSIEM)**
 - Combina información de monitorización de bases de datos con información de log de otras fuentes (Windows, Unix, firewalls, IDS, etc.)
 - Portal para seguridad y compliance a nivel de empresa
- **Nuevos gestores de bases de datos soportados**
 - PostgreSQL & Netezza
 - Complementa soporte previo de IBM DB2 and Informix, Oracle, SQL Server, Sybase, MySQL, Teradata
- **Mejoras en escalabilidad, usabilidad y rendimiento basado en feedback continuo de instalaciones actuales**





Auditoría Detallada

Todo el tráfico SQL se analiza y se filtra en tiempo real para proveer información específica a los auditores



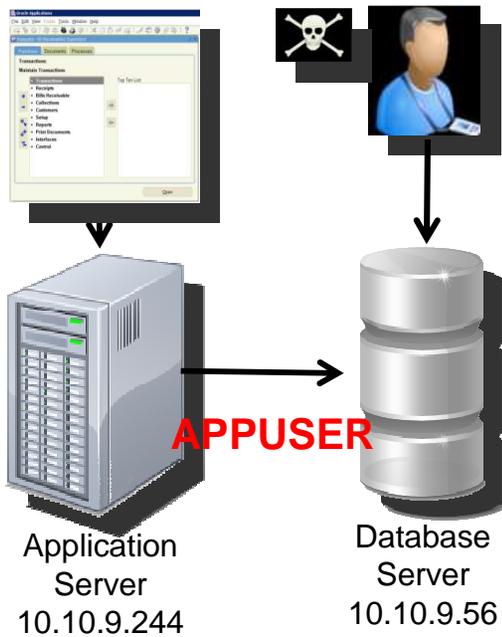
Client IP
 OS user ID
 Client host name
 Domain login
 Client OS
 MAC
 TTL
 Origin
 Failed logins

Server IP
 Server port
 Server name
 Session
 SQL patterns
 Network protocol
 Server OS
 Timestamp
 App user ID
 Access programs

ALL SQL commands
 Fields
 Objects
 Verbs
 DDL
 DML
 DCL
 DB user ID
 DB version
 DB type
 DB protocol
 Ports
 SQL errors
 SELECTs
 Bind values



Políticas Granulares con Alertas de Tiempo Real



- CIFS
- DB2
- FTP
- IBM DB2 Z/OS
- IBM ISERIES
- IMS
- Informix
- MS SQL SERVER
- MYSQL
- Oracle
- Sybase
- TERADATA

Rule #1 Description non-App Source AppUser Connection

Category Security **Classification** Breach **Severity** MED

Hot **Server IP** / and/or **Group** Production Servers

Hot **Client IP** / and/or **Group** Authorized Client IPs

Hot **Client MAC** and/or **Net. Protocol** and/or **Group**

Hot **DB Name**

Hot **DB User** APPUSER

Field Name

Object INVENTORY

Command DROP TABLE

Min. Ct. 0 **Reset Interval (minutes)** 0

Continue to next Rule **Rec. Vals.**

Action ALERT PER MATCH

Notification

Notification Type MAIL **Mail User** marc.gamache@guardium.com

ALERT DAILY
ALERT ONCE PER SESSION
ALERT PER MATCH
ALERT PER TIME GRANULARITY
ALLOW
IGNORE RESPONSES PER SESSION
IGNORE SESSION
IGNORE SQL PER SESSION
LOG FULL DETAILS
LOG FULL DETAILS PER SESSION
LOG FULL DETAILS WITH VALUES
LOG FULL DETAILS WITH VALUES PER SESSION
LOG MASKED DETAILS
LOG ONLY
RESET
S-GATE ATTACH
S-GATE DETACH
S-GATE TERMINATE
S-TAP TERMINATE
SKIP LOGGING

From: GuardiumAlert@guardium.com Sent: Wed 4/15/2009 8:00 AM
To: Marc Gamache
Cc:
Subject: (c1) SQLGUARD ALERT

Subject: (c1) SQLGUARD ALERT Alert based on rule ID non-App Source AppUser Connection
Category: security Classification: Breach Severity MED
Rule # 20267 [non-App Source AppUser Connection]
Request Info: [Session start: 2009-04-15 06:59:03 Server Type: ORACLE Client IP 192.168.20.160 ServerIP: 172.16.2.152 Client PORT: 11787 Server Port: 1521 Net Protocol: TCP DB Protocol: INS DB Protocol Version: 3.8 DB User: APPUSER
Application User Name
Source Program: JDBC THIN CLIENT Authorization Code: 1 Request Type: SQL_LANG Last Error:
SQL: select * from EmployeeTable

Auditoría y Generación de Informes (Reporting)

- **Dispone de diversos aceleradores de cumplimiento de normativas (SOX, PCI, Basilea II, HIPAA...)**
 - Monitorización de aplicaciones financieras (EBS, JD Edwards, PeopleSoft, etc)
 - Sólo acceso de aplicación autorizado
 - Informes de cumplimiento automatizados, revisión, firma y escalado (SOX, PCI, NIST, etc.)

PCI Accelerator 

Overview | REG 3 Protect  | REG 6 Maintain | REG 7 Restrict | REG 8 Assign | PCI Req. 10 Track & Monitor | REG 11 Test | PCI Policy Monitoring

Overview

Cardholder Server IPs List

Cardholders DBs

Cardholder Objects

Data Access Map

DB Clients to Servers Map

Active DB Users

Cardholder DB Administration

Source Programs

Review Groups

PCI - Cardholder Server IPs

Start Date: 2007-01-01 00:00:00 End Date: 2007-05-31 00:00:00

Server IP	Server Type	Database Name	Count of Sessions
192.168.1.186	ORACLE	CARD_DATA	8
192.168.2.51	ORACLE	CARD_DATA	140
192.168.200.108	DB2	CARD_DATA	182
192.168.200.108	DB2	DN8DEMO3	258
192.168.200.108	DB2	SAMPLE	44

Descubrimiento de Bases de Datos y Clasificación de Datos Sensibles

- ✓ Descubrimiento de bases de datos
- ✓ Descubrimiento de datos sensibles
- ✓ Acciones basadas en políticas
 - *Alertas*
 - *Añadir a un grupo de objetos sensibles*

Administration Console | Access Management | Tools | Daily Monitor | SQL Guard Monitor | Tap Monitor | Incid

SQL Count
Session Count
Logged Threshold Alerts
Logged R/T Alerts
Exception Count
Dropped Requests
TCP Exceptions
Admin User Logins
Databases by Type
Databases Discovered
Retrospective Report Requests
Values Changed
Throughput

Databases Discovered

Start Date: 2008-06-26 14:48:49 End Date: 2008-06-26 15:48:49

Time Probed	Server IP	Server Host Name	DB Type	Port	Port Type	#
2008-06-26 15:31:00	10.10.9.253	10.10.9.253	Oracle	1521	tcp	1
2008-06-26 15:30:58	10.10.9.253	10.10.9.253	MSSQL	1433	tcp	1
2008-06-26 15:30:15	10.10.9.55	osprey	Oracle	1521	tcp	1
2008-06-26 15:30:15	10.10.9.55	osprey	Sybase	4200	tcp	1
2008-06-26 15:30:32	10.10.9.56	10.10.9.56	Oracle	1521	tcp	1
2008-06-26 15:30:58	10.10.9.56	10.10.9.56	DB2	50001	tcp	1

https://10.10.9.242:8443/viewClsProcessResult.do?method=view&viewerType=assessmentResults&viewe - Internet Explorer provided by

https://10.10.9.242:8443/viewClsProcessResult.do?method=view&viewerType=assessmentResults&viewedTaskId=-1&noButtons=false&selectedProcessId=20016

Catalog	Schema	Table Name	Column Name	Rule Description	Comments	Classification Name	Category	Data Source Description
<input type="checkbox"/>	BANKAPP	CREDITCARD	CARDNUMBER	Send Alert	Date: Monday, July 21, 2008 6:30:07 PM EDT Datasource: ORACLE 10.10.9.56:1521 xe Object: TABLE BANKAPP.CREDITCARD VARCHAR2 (20) CARDNUMBER Category: 'PCI' Classification: 'Cardholder Data' Rule: Search For Data: Send Alert TABLE_TYPE='TABLE,VIEW', DATA_TYPE='TEXT', SEARCH_VALUE_PATTERN='[0-9]{4}-[0-9]{4}-[0-9]{4}-[0-9]{4}' Action: Send Alert: Send Alert Urgent Flag='false', Receiver='SYSLOG' Action: Log Policy Violation: Send Policy Violation Severity='10' Action: Add To Group Of Objects: add to group Object Group='PCI Cardholder Sensitive objects', Replace Group Content='false'	Cardholder Data	PCI	10-56-system

Evaluar y Reforzar – Análisis de Vulnerabilidades (VA)

- Basados en estándares reconocidos tales como STIG y CIS benchmark tests.
- Cobertura completa del entorno global de las bases de datos:
 1. *Comportamiento Observado*
 2. *Bases de Datos*
 3. *Sistema Operativo*

Tests passing: **38%**

Based on the tests performed under this assessment, data access of the defined database environments requires improvement. Refer to the recommendations of the individual tests to learn how you can address problems within your environment and what you should focus upon first. Once you have begun addressing these problems you should also consider scheduling this assessment as an audit task to continuously assess these environments and track improvement.

[View log](#)

[Jump to Datasource list](#) 

Result Summary *Showing 93 of 93 results (0 filtered)*

	Critical	Major	Minor	Caution	Info
Privilege	8p 16f	2p 3f	-- 2f	-- --	-- --
Authentication	-- 6f	-- 1f	-- 1f	-- --	-- --
Configuration	2p 2f	5p 6f 4e	2p 2f 4e	-- 6f 1e	-- 1f
Version	-- --	-- 2f	-- --	-- --	-- --
Other	1p	-- 3p 2f	3p 1f	-- --	-- 6p 1f

VA Configuración – Selección de Tests

IBM InfoSphere Guardium (g8) - Mozilla Firefox: IBM Edition

10.10.9.248 https://10.10.9.248:8443/sqlguard/media-type/html/user/admin/page/default.psm/js_pane/P-12aabfabd49-1002c

IBM InfoSphere Guardium (g8)

IBM InfoSphere™ Guardium® 16:56 | [Edit Account](#)

You have 4 items on your To-do list

System View Administration Console Tools **Daily Monitor** Guardium Monitor Tap Monitor Incident Management My New Reports

Config & Control

- Access Map Builder/Viewer
- Alert Builder
- Alias Builder
- Audit Process Builder
- Audit Process To-do List
- Auto-discovery Configuration
- Baseline Builder
- CAS Host Config
- CAS Template Set Config
- Classification Policy Builder
- Classification Process Builder
- Datasource Definitions
- Group Builder
- Policy Builder
- Portlet Editor
- Privacy Set Builder
- Security Assessment Builder**
- Time Period Builder
- Value Change Audit DB Creation
- Value Change Audit DB Update & Upload
- Value Change Auditing Builder
- Workflow Builder

Security Assessment Builder

Assessment Test Selections

Tests for Security Assessment VA Test for Systemz - DB1S (Subset)

Select All Unselect All Delete Selected

Type	Test Name	Tuning
<input type="checkbox"/> DB2	z/OS Restrict system privilege - ARCHIVEAUTH	PRIV Critical (n/a) :
<input type="checkbox"/> DB2	z/OS Restrict system privilege - BINDADDAUTH	PRIV Critical (n/a) :
<input type="checkbox"/> DB2	z/OS Restrict system privilege - BINDAGENTAUTH	PRIV Critical (n/a) :
<input type="checkbox"/> DB2	z/OS Restrict system privilege - BSDSAUTH	PRIV Critical (n/a) :
<input type="checkbox"/> DB2	z/OS Restrict system privilege - CREATEALIASAUTH	PRIV Critical (n/a) :
<input type="checkbox"/> DB2	z/OS Restrict system privilege - CREATEDBAAUTH	PRIV Critical (n/a) :
<input type="checkbox"/> DB2	z/OS Restrict system privilege - CREATEDBCAUTH	PRIV Critical (n/a) :
<input type="checkbox"/> DB2	z/OS Restrict system privilege - CREATECSAUTH	PRIV Critical (n/a) :

Tests available for addition Predefined Query based CVE All

[Observed] **DB2** INFORMIX MS SQL SERVER MYSQL NETEZZA ORACLE POSTGRESQL SYBASE TERADATA

Tests marks with an asterisk (*) require specific CAS monitoring running on the Datasource(s) tested

VER: Version: DB2
 PRIV: z/OS Grant option - Package
 PRIV: z/OS Grant option - Plan
 PRIV: z/OS Grant option - Resauth
 PRIV: z/OS Grant option - Routine
 PRIV: z/OS Grant option - Schema
 PRIV: z/OS Grant option - Sequence
 PRIV: z/OS Grant option - Table and View
 PRIV: z/OS Grant to PUBLIC - Column
 PRIV: z/OS Grant to PUBLIC - Package
 PRIV: z/OS Grant to PUBLIC - Plan

Add Selections

Groups Save Back

VA for DB2 z/OS – Ejemplo de resultados

Tests passing: **97%***
*Percentage does not take into account any current filtering

Based on the tests performed under this assessment, data access of the defined database environments conform to best practices. You have a controlled environment in terms of the tests performed. You should consider scheduling this assessment as an audit task to continuously assess these environments.

Result Summary Showing 59 of 59 results (0 filtered)

	Critical	Major	Minor	Caution	Info
Privilege 48p 2f -- 8p					
Authentication --					
Configuration 1p					
Version --					
Other --					

Current filtering applied:
 Test Severities: - Show All -
 Datasource Severities: - Show All -
 Scores: - Show All -
 Types: - Show All -

Assessment Test Results Showing 59 of 59 results (0 filtered)

Test / Datasource	Result
z/OS Restrict system privilege - SYSADMAUTH Test category: Priv. Severity: Critical The SYSADMAUTH privilege grants the authority to a grantee with system administration authority. It is recommended that SYSADMAUTH privilege be granted to authorize users only. This test exclude grantee who is a member of SYSADM. Ext. Reference: Guardium, Test ID 2164	Fail SYSADM privilege has been granted to unauthorized users. Recommendation: We recommend you revoke SYSADMAUTH from unauthorized grantee. You can use this command to revoke: REVOKE SYSADM FROM <grantee> BY ALL. To exclude authorize SYSADMAUTH grantee, you can create a group then populate it with authorize grantee and link your group to this test.

z/OS Grant option - Routine
 Test category: Priv. Severity: Critical
 This test check for object privileges on routines that has been granted with the grant option. A routine can be a user-defined function, cast function, or stored procedure. Grant option is not a good practice and should be avoid where possible. When object privileges are granted with the grant option, a user can grant privileges on that object to other users. We do not recommend granting objects privilege with grant option. This test exclude grantee who is a member of SYSADM and SYSIBM user. Grantee type 'P' is also excluded from this test.
 Ext. Reference: Guardium, Test ID 2180

DPS: DB2 z/OS 9.1 rocket
 Datasource type: DB2 Severity: None

Details: Grantee causing failure:

z/OS Grant option - Schema
 Test category: Priv. Severity: Critical
 This test check for schema privileges that has been granted with the grant option. Grant option is not a good practice and should be avoid where possible. When object privileges are granted with the grant option, a user can grant privileges on that object to other users. We do not recommend granting objects privilege with grant option. This test exclude grantee who is a member of SYSADM and SYSIBM user.
 Ext. Reference: Guardium, Test ID 2181

DPS: DB2 z/OS 9.1 rocket
 Datasource type: DB2 Severity: None

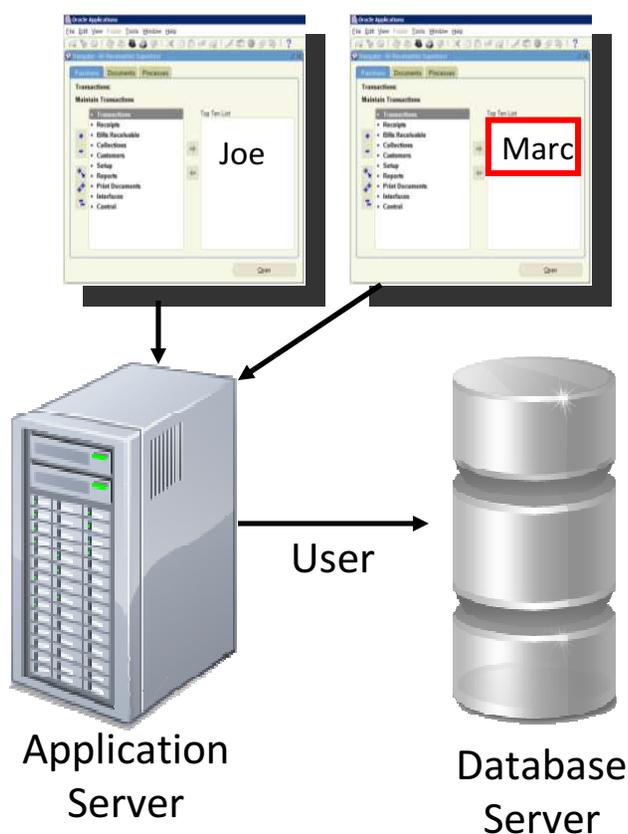
Details: Grantee causing failure:

z/OS Grant option - Sequence
 Test category: Priv. Severity: Critical
 This test check for object privileges on sequences that has been granted with the grant option. Grant option is not a good practice and should be avoid where possible. When object privileges are granted with the grant option, a user can grant privileges on that object to other users. We do not recommend granting objects privilege with grant option. This test exclude grantee who is a member of SYSADM and SYSIBM user. Grantee type 'P' is also excluded from this test.
 Ext. Reference: Guardium, Test ID 2182

Recomendaciones tras evaluación de Vulnerabilidades

Assessment Test Results		Compare with Previous Results			<i>Showing 93 of 93 results (0 filtered)</i>
Cat.	Test Name	Datasource	P/F	Sev.	Reason
Conf.	DBA Profile PASSWORD LIFE TIME Is Limited	ORACLE: Oracle on Ocean	Fail	Critical	User profile [DEFAULT] setup parameter PASSWORD_LIFE_TIME found out of defined threshold value <i>Recommendation: The PASSWORD_LIFE_TIME parameter is not set, allowing users to retain the same password indefinitely. Passwords that have been in use for long periods of time ar likely to become known to unauthorized users. We recommend that you set this parameter in order to limit the lifetime of users' passwords.</i>
Conf.	DBA Profile PASSWORD VERIFY FUNCTION Is Implemented	ORACLE: Oracle on Ocean	Fail	Critical	Found active profile 'APPL_PROFILE, DEFAULT' with PASSWORD_VERIFY_FUNCTION not implemented <i>Recommendation: No Password Verification Routine has been implemented. We recommend that you implement a password function to prevent the use of weak passwords.</i>
Auth.	Default Accounts Password Changed	ORACLE: Oracle on Ocean	Fail	Critical	2 active pre-defined users have default passwords. <i>Recommendation: Some predefined Oracle user accounts are still enabled and still have the Oracle default password. These predefined Oracle users and passwords are well-known to anyone familiar with Oracle, and represent one of the easiest entry points for attacks and data theft/damage. We recommend that your remove any predefined Oracle user accounts that are not absolutely required, and we strongly recommend that you change the passwords for any of these users who are required.</i>
Priv.	No Access To 'Users' Catalog Tables	ORACLE: Oracle on Ocean	Fail	Critical	Some users or roles without 'SELECT_CATALOG_ROLE' authority have access to 'DBA_USERS' or 'ALL_USERS': CTXSYS, PUBLIC. <i>Recommendation: Access to the DBA_USERS or ALL_USERS tables has been granted to users other than DBA or SELECT_CATALOG_ROLE. We recommend restricting access to these tables for security reasons.</i>

Identificación del fraude en la capa de aplicación

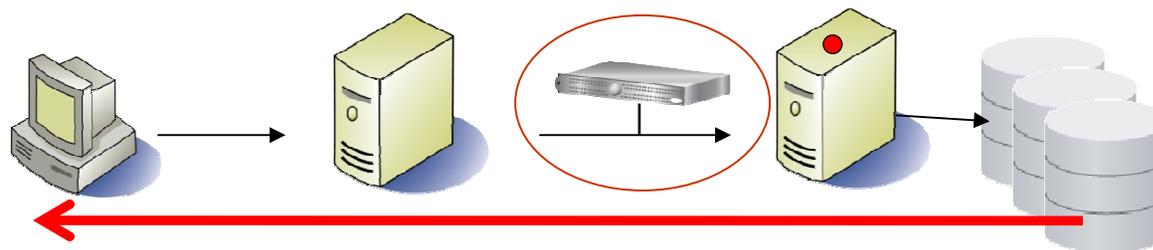


DB User Name	Application User	Sql
APPUSER	joe	select * from EmployeeRoleView where UserName=?
APPUSER	joe	select * from EmployeeTable
APPUSER	marc	insert into EmployeeTable values (?,?,?,?,?,?,?)

- **Problema:** el servidor de aplicaciones usa una cuenta genérica de servicio para acceder a las bases de datos
 - **No identifica quién** inició la transacción (connection pooling)
- **Solución:** Guardium realiza seguimiento del acceso al **usuario de aplicación asociado con comandos SQL específicos**
 - Soporte incluido para la mayoría de las aplicaciones empaquetadas de empresas (Oracle EBS, PeopleSoft, SAP, Siebel, Business Objects, Cognos...) y aplicaciones propias (WebSphere...)



Monitorización de Fuga de Información



¿Es correcto esto?

DB User Name	Sql	Records
STEVE	select * from ar.creditcard where i>? and i<? 4	4
HARRY	select * from ar.creditcard where i<?	4
JOE	select * from ar.creditcard where i<?	99

¿Qué fue lo que vio?

HARRY	select * from ar.creditcard where i<?	*****0002, *****0003, *****0004
JOE	select * from ar.creditcard where i<?	*****0001
JOE	select * from ar.creditcard where i<?	*****0002, *****0003, *****0004, *****0005, *****0006, *****0007, *****0008, *****0009, *****0010, *****0011, *****0012, *****0013, *****0014, *****0015, *****0016
JOE	select * from ar.creditcard where i<?	*****0017, *****0018, *****0019, *****0020, *****0021, *****0022, *****0023, *****0024, *****0025, *****0026, *****0027, *****0028, *****0029, *****0030, *****0031
JOE	select * from ar.creditcard where i<?	*****0032, *****0033, *****0034, *****0035, *****0036, *****0037, *****0038, *****0039, *****0040, *****0041, *****0042, *****0043, *****0044, *****0045, *****0046
JOE	select * from ar.creditcard where i<?	*****0047, *****0048, *****0049, *****0050, *****0051, *****0052, *****0053, *****0054, *****0055, *****0056, *****0057, *****0058, *****0059, *****0060, *****0061
JOE	select * from ar.creditcard where i<?	*****0062, *****0063, *****0064, *****0065, *****0066, *****0067, *****0068, *****0069, *****0070, *****0071, *****0072, *****0073, *****0074, *****0075, *****0076
JOE	select * from	*****0077, *****0078, *****0079, *****0080, *****0081, *****0082

Workflow: Firmas y Escalados automatizados



Guardium

Weekly Database Change Management Process
Audit process execution began 4/16/09 12:24 AM

Other Results For This Process [v] [?]

Sign Results Continue Escalate Comment Download PDF

Distribution Status: [+]
Comments: [x]

Timestamp	User	Comment for Result
2009-04-16 00:42:37.0	Marc	Need to review the DB login failure more closely! App User account should not fail a login.

[+] [Report: Database Changes Report \[-ChangeRequest Report\] Overall Value: 3](#)

[+] [Security Assessment: Security Assessment \[-Assessment\] Overall Value: 36](#)

[+] [Classification Process: Classification Process \[Search for CreditCard Accounts - CreditCard Accounts\]](#)

[+] [Report: Failed DB Logins Report \[Failed User Login Attempts\] Overall Value: 1](#)

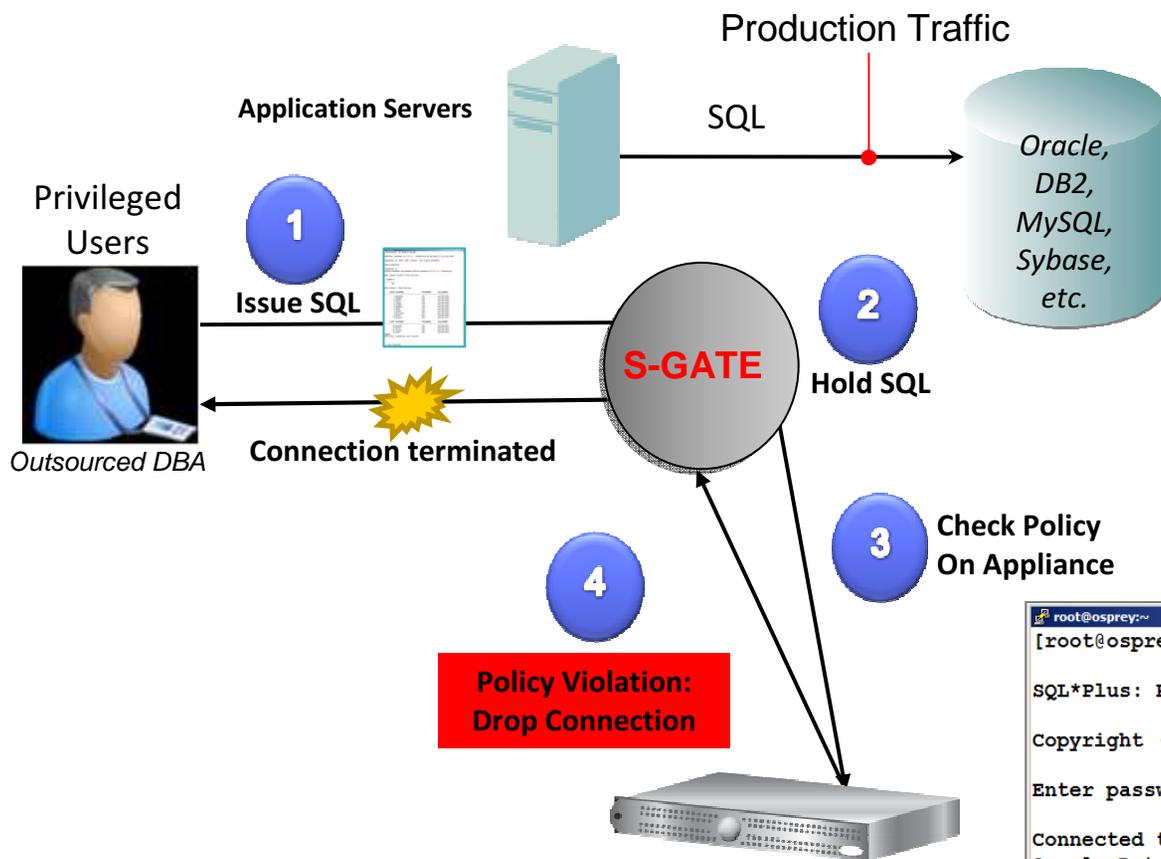
[+] [Report: SQL Errors Report \[SQL Errors\] Overall Value: 56](#)

[Close this window](#) View

- **Automatiza el flujo completo (workflow) de compliance**
 - *Distribución de informes al equipo revisor*
 - *Firma electrónica*
 - *Escalados*
 - *Comentarios y manejo de excepciones*
- **Ayuda a los auditores a documentar los procesos de revisión de documentos**
- **Los resultados del proceso de auditoría se almacenan con datos de auditoría en un repositorio seguro**
- **Centraliza y simplifica el proceso de compliance**



Prevenir de manera proactiva violaciones de políticas en tiempo real



- ✓ Sin cambios en las bases de datos
- ✓ Sin cambios en las aplicaciones
- ✓ Sin riesgo de appliances inline que puedan interferir con el tráfico de aplicaciones
- ✓ Políticas Cross-DBMS
- ✓ Bloqueo de acciones de usuarios privilegiados

```

root@osprey:~# sqlplus system
SQL*Plus: Release 10.2.0.1.0 - Production on Tue May 27 01:13:32 20
Copyright (c) 1982, 2005, Oracle. All rights reserved.

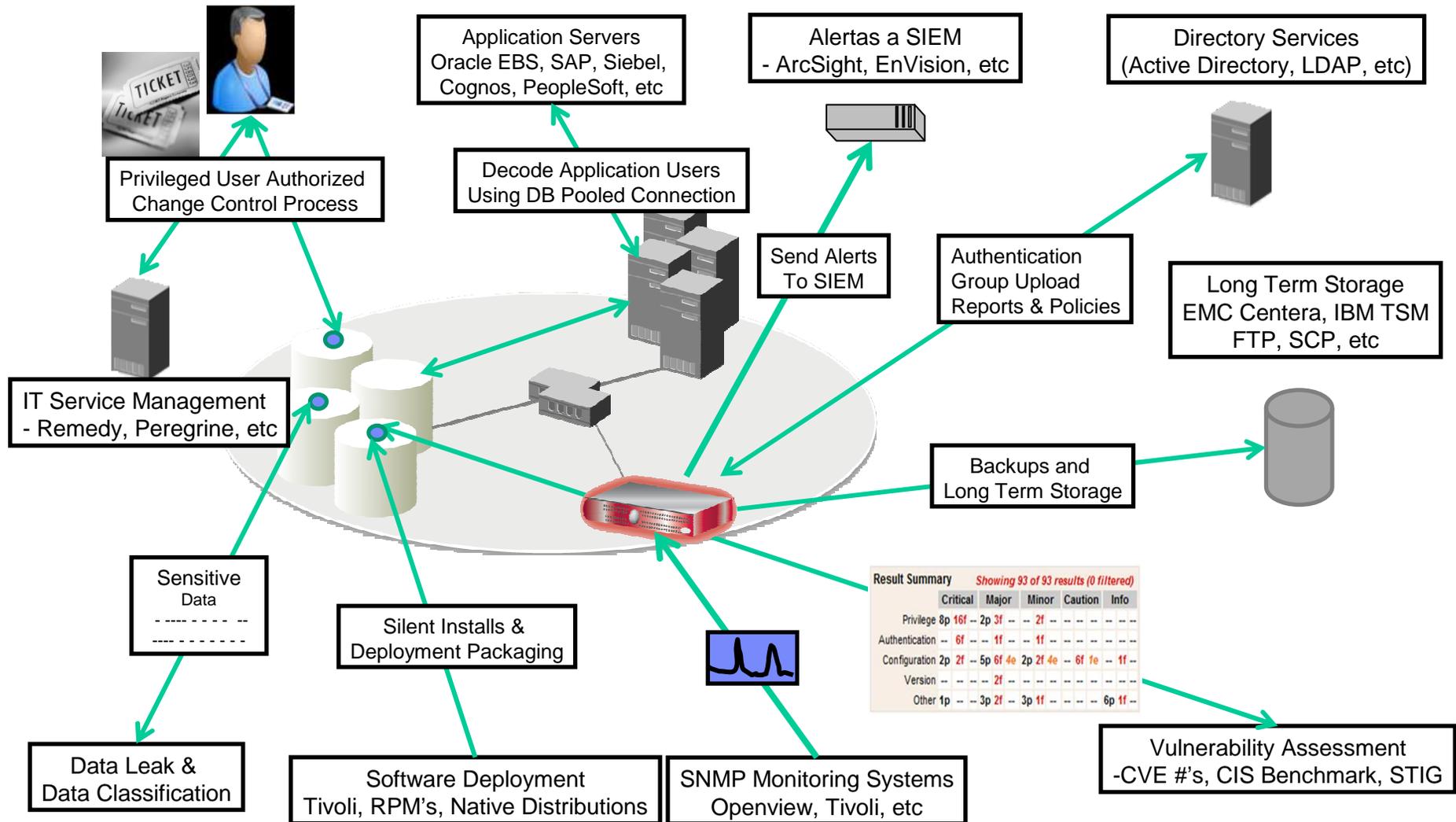
Enter password:

Connected to:
Oracle Database 10g Express Edition Release 10.2.0.1.0 - Production

SQL> select * from creditcard;
select * from creditcard
*
ERROR at line 1:
ORA-03113: end-of-file on communication channel

Session Terminated
SQL>
    
```

Integración con Infraestructura Existente



Requisitos del Auditor: Planificar, Proteger y Auditar

■ Acceso a datos

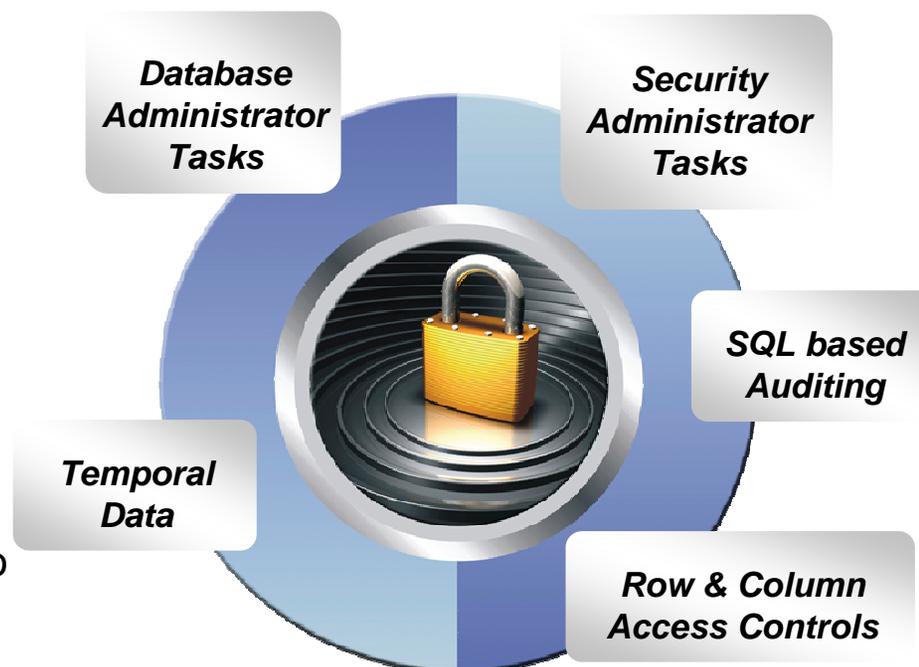
- Minimizar el uso de autorizaciones de superusuario tales como SYSADM
- Un grupo, que no sea el propietario de los datos, debería gestionar el acceso a datos restringidos

■ Auditoría de datos

- Cualquier acceso dinámico o uso de una autorización privilegiada necesita ser auditada
- Conservar y gestionar los datos de auditoría por largos periodos de tiempo (según normativas)

■ Privacidad de datos

- Todo el acceso dinámico a las tablas que contengan información restringida, debe ser protegida



*Today's Mainframe:
The power of industry-leading security,
the simplicity of centralised management*

Roles que intervienen en Monitorización y Auditoría



OPERACION DE SEGURIDAD

- ✓ Políticas Tiempo Real
- ✓ Rastro seguro de auditoría
- ✓ Bloqueo a información sensible
- ✓ Minería de datos & forense



CUMPLIMIENTO DE AUDITORÍA

- ✓ Segregación de tareas
- ✓ Informes de Mejores Prácticas
- ✓ Controles Automatizados

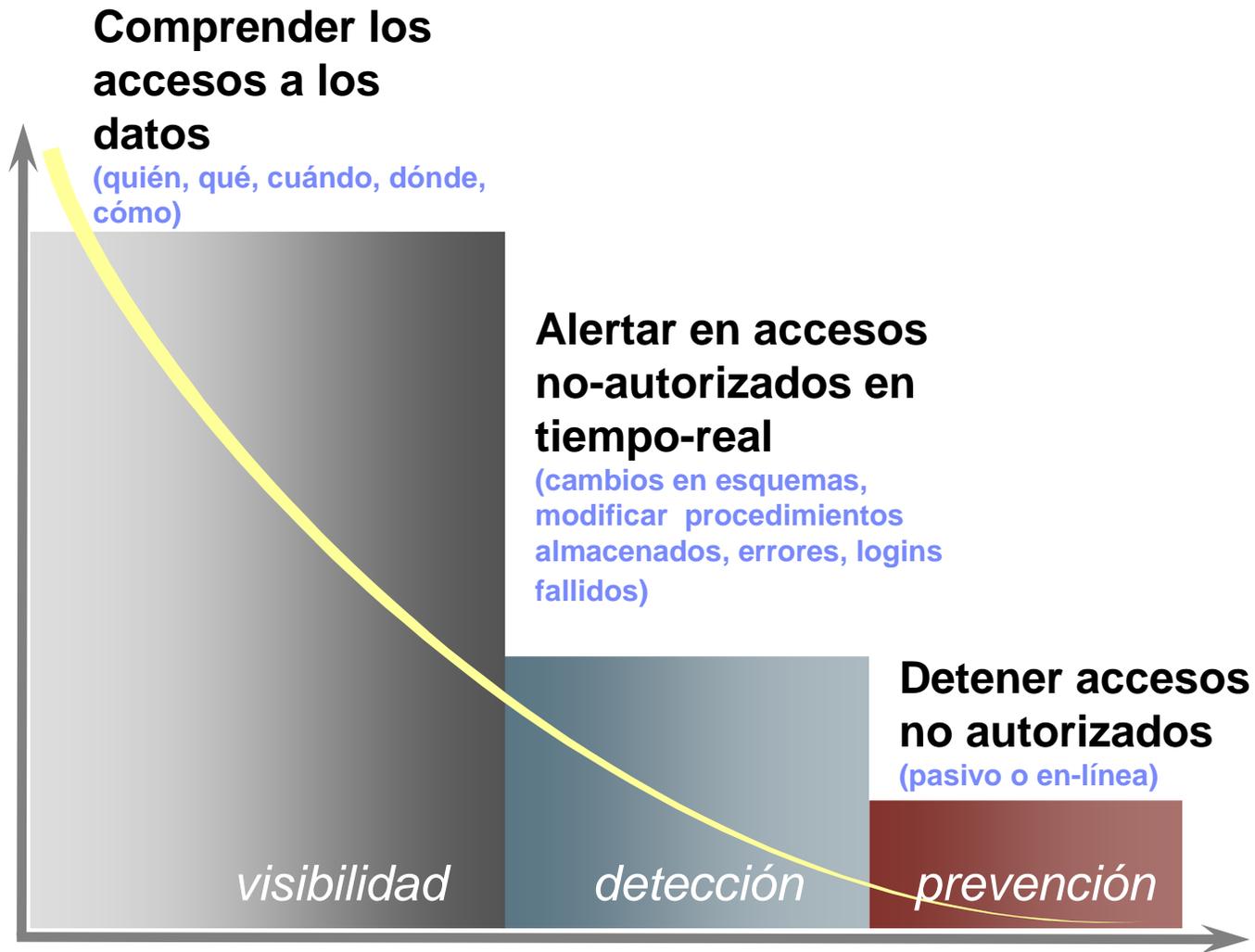


BASES DE DATOS Y APLICACIONES

- ✓ Impacto Mínimo
- ✓ Administración de Cambios
- ✓ Optimización de Rendimiento
- ✓ Parches y Configuración

**Guardium: 100% Visibilidad &
Visión Unificada**

Implantación por fases





Características de Guardium for z

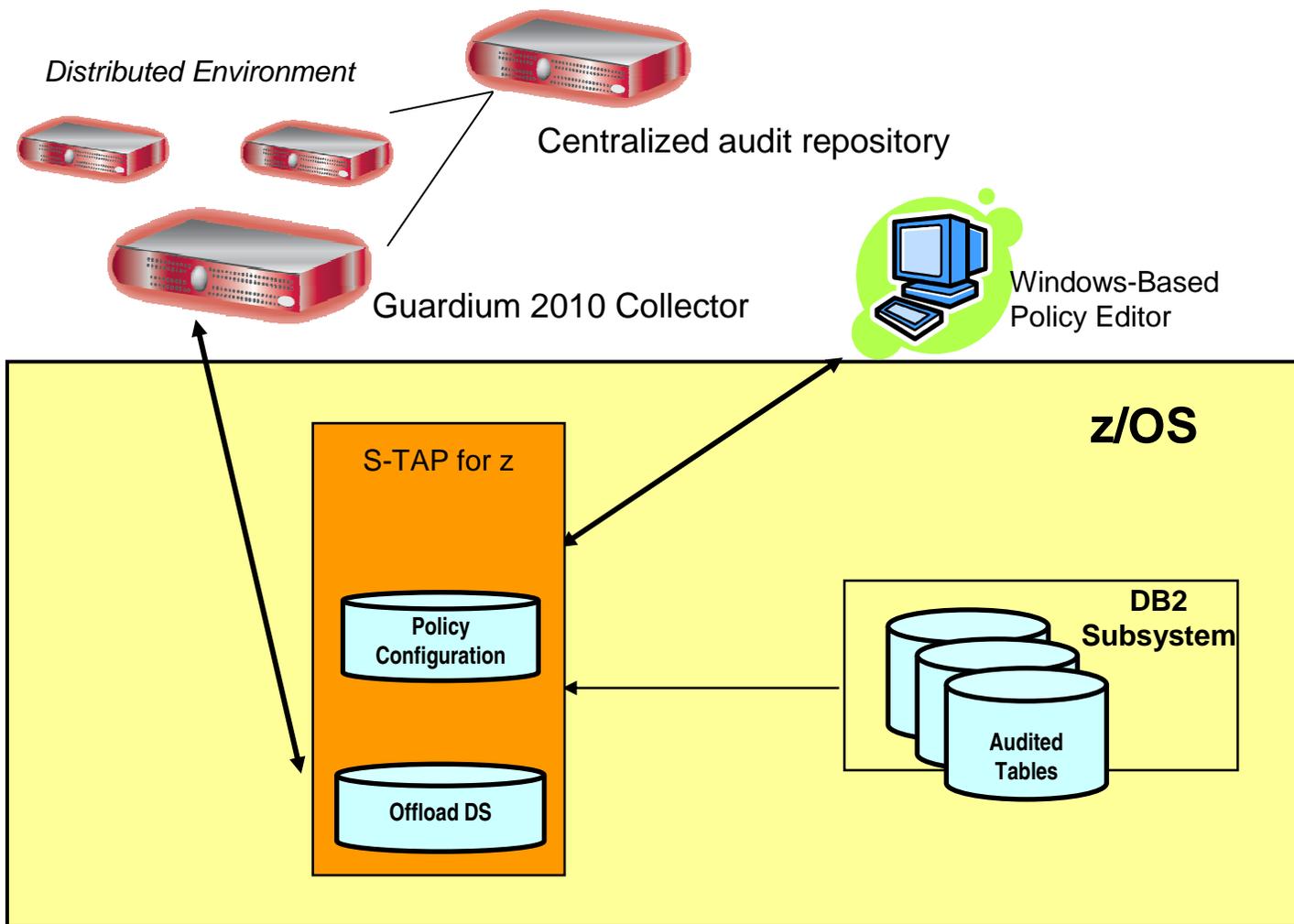
- Proporciona una **vista unificada** y un registro seguro de actividades de auditoría para todas las acciones relacionadas con bases de datos – cubre entornos mainframe y distribuidos
 - Proporciona informes de cumplimiento a nivel de empresa, análisis y diagnóstico forense
- Puede ser gestionada por auditores (no DBAs), favoreciendo la **segregación de roles**
- Reduce los costes de cumplimiento y el esfuerzo a través de **controles automatizados y centralizados** (vs. procesos manuales y ad hoc)
 - Con automatización de un workflow de cumplimiento (firmas, escalados, ...)
- Aprovecha la tecnología IBM disponible en el mainframe
- Impacto mínimo en rendimiento



Características de Guardium for z

- **Utiliza la mejor tecnología de captura de eventos de DB2 en z/OS**
 - Despliegue con poco impacto
 - Datos de auditoría enviados al *Guardium appliance*, pueden aislarse del subsistema auditado
 - No necesita utilizar las clases 4 y 5 de la traza de audit
 - Inversión permanente del laboratorio en mejoras de rendimiento y de recogida de datos para adaptarse a los requisitos de clientes
 - Óptimo rendimiento para clientes que utilizan el IBM Query Monitor
 - La monitorización de queries y los requisitos de auditoría aprovechan un mismo colector de procesos
- **Emplea la mejor tecnología de seguridad de bases de datos de Guardium**
 - Aprovecha la funcionalidad off-host de Guardium
- **Se integra dentro del entorno Guardium de auditoría del resto de gestores de bases de datos existentes en la empresa**
 - Reporting y alertas unificados, agregación centralizada de datos de auditoría

Guardium for z –Arquitectura



Ejemplo de Información de Auditoría registrada

The screenshot displays two windows. The top window, titled 'Full SQL LIKE', shows a table of query execution records. The bottom window, titled 'Vista TN3270 Session B', shows a terminal window with a JCL job definition and its execution output.

Full SQL ID	Timestamp	Service Name	DB User Name	OS User	Session Start	Source Program	Full Sql	Client IP
18800880	2008-08-22 14:01:34.0	DGA4/DGA	CFP2/CFP2	CFP2	2008-08-22 14:01:33.0	DSNTEP2	SELECT * FROM SYSIBM.SYSTABLES WHERE OWNER = 'SYSDSN'	10.37.100.29

The terminal window shows the following JCL job definition and execution output:

```

EDIT      NSU.CFP.JCLLIB(DSNTEP2) - 01.13      Columns 00001 00072
Command ==> SUBMIT
***** Top of Data *****
000100 //DSNTEP2  JOB (ACCT),' ,MSGCLASS=X,NOTIFY=&SYSUID
000110 //*
000131 /*JOBPARM SYSAFF=*
000132 //*
000140 //*****
000150 //SQL      EXEC PGM=IKJEFT01,DYNAMNBR=20,TIME=15,REGION=0M
000160 //*****
000170 //*
000171 //STEPLIB DD DSN=SYS3.DGA.SDSNEXIT,DISP=SHR
000172 //          DD DSN=DSN810.SDSNLOAD,DISP=SHR
000190 //*
000200 //SYSTSPR DD SYSOUT=*
000300 //SYSPRINT DD SYSOUT=*
000400 //SYSTSI  DD *
000500 DSN=SYS3.DGA.SDSNEXIT
000600 RUN PROGRAM (DSNTEP2) -
000700 LIB('SYS3.DSN810.RUNLIB.LOAD')
000800 /*
000900 //SYSIN   DD *
000901 SELECT * FROM SYSIBM.SYSTABLES WHERE OWNER = 'SYSDSN';
***** Bottom of Data *****
    
```

Red arrows point from the terminal window to the table above. One arrow points from the 'Source Program' column to the 'DSNTEP2' entry in the JCL. Another arrow points from the 'Full Sql' column to the 'SELECT * FROM SYSIBM.SYSTABLES WHERE OWNER = 'SYSDSN'' entry in the JCL. A third arrow points from the 'Full Sql' column to the 'SELECT * FROM SYSIBM.SYSTABLES WHERE OWNER = 'SYSDSN'' entry in the table. Red boxes highlight the 'DSN=SYS3.DGA.SDSNEXIT' and 'SELECT * FROM SYSIBM.SYSTABLES WHERE OWNER = 'SYSDSN'' lines in the terminal output.

Ejemplo de Informe de datos de Auditoría en Guardium

Local DB2 Traffic

Job ID (Source Program)

RACF ID/SQL ID

SQL with Bind Values

SQL with Redacted Values

DRDA Traffic (Network)

Timestamp	Server Type	Client IP	Server IP	Network Protocol	Source Program	DB User Name	OS User	Full Sql	Sql
2008-07-08 05:41:43.0	DB2	10.37.100.26	10.37.100.26	LOCAL	NSUQAG	NESQA/NESQA	NESQA	SELECT STMT INTO 'GASSPO40' FROM SYSIBM . SYSPACKSTMT WHERE COLLID = 'GASSPO40' AND NAME = '	SELECT STMT INTO 'GASSPO40' FROM SYSIBM . SYSPACKSTMT WHERE COLLID = ? AND NAME = ? AND CONTOKEN = ? AND STMTNO = : H
2008-07-08 05:41:43.0	DB2	10.37.100.26	10.37.100.26	LOCAL	NSUQAG	NESQA/NESQA	NESQA	SELECT STMT INTO : H FROM SYSIBM . SYSPACKSTMT WHERE COLLID = : H AND NAME = : H AND CONTOKEN = : H AND STMTNO = : H	SELECT STMT INTO : H FROM SYSIBM . SYSPACKSTMT WHERE COLLID = : H AND NAME = : H AND CONTOKEN = : H AND STMTNO = : H
2008-07-08 05:41:43.0	DB2	11.100.37.10	10.37.100.26	TCP	DGD1DIST	SAS1/SAS1	DGD1DIS	RELEASE TO SAVEPOINT Q4_SP	RELEASE TO SAVEPOINT Q4_SP
2008-07-08 05:41:37.0	DB2	11.100.37.10	10.37.100.26	TCP	DGD1DIST	SAS1/SAS1	DGD1DIS	DELETE FROM NSUQA1.EMP_RESUME WHERE EMPNO = 'TSTQ40'	DELETE FROM NSUQA1 . EMP_RESUME WHERE EMPNO = ?

Ejemplo de informe de auditoría (continuación)

- SQL Trace						
Start Date: 2010-06-07 15:09:45 End Date: 2010-06-08 18:09:45						
Aliases: OFF CLIENTIP: LIKE %						
DBUSER: LIKE % FULLSQL: LIKE %						
SEVERIP: LIKE % SQL: LIKE %						
Timestamp	Client IP	Server IP	Server OS	DB User Name	OS User	Sql
2010-06-08 03:11:24.015.22.19.50	RL25	Z/OS	GU0002	GU0002	REVOKE EXECUTE ON PROCEDURE SYSIBM.SQLTABLEPRIVILEGES FROM PUBLIC BY ALL RESTRICTI	
2010-06-07 22:12:28.015.22.19.50	RL25	Z/OS	GU0001	GU0001	INSERT INTO udt_table VALUES(CAST(? AS udt1), CAST(? AS udt2), CAST(? AS udt3))	
2010-06-08 03:04:29.015.22.19.50	RL25	Z/OS	GU0001	GU0001	INSERT INTO udt_table VALUES(CAST(? AS udt1), CAST(? AS udt2), CAST(? AS udt3))	
2010-06-07 22:14:09.015.22.19.50	RL25	Z/OS	GU0001	GU0001	delete from camp_roster where NAME like ?	
2010-06-08 03:12:13.015.22.19.50	RL25	Z/OS	GU0002	GU0002	GRANT CREATEIN,ALTERIN,DROPIN ON SCHEMA va_test_schema TO QA_TEST	
2010-06-08 03:11:10.015.22.19.50	RL25	Z/OS	GU0002	GU0002	REVOKE EXECUTE ON PACKAGE NULLID.SYSSN101 FROM PUBLIC BY ALL	
2010-06-08 02:29:05.015.22.19.50	RL25	Z/OS	GU0002	GU0002	GRANT ALL ON TABLE VA_TEST EMP TO VA_TEST	

Alertas

- Los datos de auditoría procesados pueden generar alertas

Policy Violations / Incident Management

Start Date: ~~2010-06-01 10:09:28~~ End Date: 2010-06-09 10:09:28

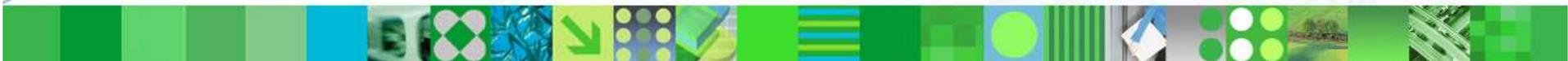
Aliases: ON

<u>Violation Log Id</u>	<u>Timestamp</u>	<u>Category Name</u>	<u>Access Rule Description</u>	<u>Client IP</u>	<u>Server IP</u>	<u>DB User Name</u>	<u>Full SQL String</u>	<u>Severity Description</u>
6	2010-06-08 18:46:11.0		Alert on DML	10.10.10.50	10.10.9.32	GU0001	DELETE FROM GU0001.US_SALES1 WHERE INVOICE#=1	INFO
5	2010-06-08 18:45:08.0		Alert on DML	10.10.10.50	10.10.9.32	GU0001	INSERT INTO GU0001.US_SALES1 (INVOICE#, CUST_ID, SALE_VALUE, SALE_INSERT_TS, SALE_UPDATE_TS) VALUES (7,300 ,3545.33 , '2010-06-08 18:31:46.813102','2010-06-08 18:31:46.813102')	INFO

Cómo ayuda Guardium al cumplimiento con PCI-DSS

Req. Description	Guardium PCI Capabilities
2 Do not use vendor defaults for system passwords <ul style="list-style-type: none"> • Configure system parameters to prevent misuse • Encrypt non-console admin access 	Comprehensive suite of DBMS-specific tests based on industry standards (CIS, STIG) <ul style="list-style-type: none"> • Checks for default passwords, unpatched systems, misconfigured privileges, etc. • Audits usage and alerts on misuse • Locks configurations after vulnerabilities remediated • Monitors encrypted traffic (Oracle ASO, SSL, etc.) without need for key storage
3 Protect stored cardholder data	Real-time, database leak prevention <ul style="list-style-type: none"> • Continuous, real-time, policy-based monitoring with proactive security (alerts, blocking) • Compensating control for column-level encryption • Auto-discovers & classifies stored data; identifies sensitive data in query result stream
6 Maintain secure systems <ul style="list-style-type: none"> • Establish a process to identify security vulnerabilities • Follow change control procedures for all configuration changes • Separation of duties (development, test and production) 	Centralized vulnerability and configuration assessment <ul style="list-style-type: none"> • Ensures current patches applied & vulnerable SPs identified; "virtual patching" • Alerts on all configuration changes, inside and outside databases • Enforces separation of duties with real-time alerting and granular access controls
7 Restrict access to cardholder data	Proactive, real-time access control (independent of native DBMS controls) <ul style="list-style-type: none"> • Policies defined by source IP or application, OS or DB user, time, SQL command, object, etc. • Blocks any unauthorized user, including administrators, from accessing cardholder data • Compensating control for unsegmented networks
8 Assign a unique ID to each person with computer access <ul style="list-style-type: none"> • Enforce password policies • Limit repeated access attempts 	Complements native DBMS controls with external, cross-DBMS controls <ul style="list-style-type: none"> • Alerts on credential sharing, failed logins, account creation, privilege escalation • Verifies password policies are enforced; can lock accounts or terminate sessions
10 Track and monitor access to cardholder data	Continuous, granular auditing with scalable architecture to handle high transaction volumes <ul style="list-style-type: none"> • Fine-grained audit trail of all database activities (SELECT, DDL, DML, DCL, logins, logouts, etc.) • Does not rely on native trace or audit logs: minimal perf. impact (2-3%), enforces sep. of duties • Tracks all network and local connections, including direct access by DBAs (shared memory, etc.) • Audit information stored securely in hardened appliance to prevent anti-forensics or tampering • Identifies fraud by resolving end-user IDs in connection-pooling apps (SAP, Cognos, PeopleSoft, etc.) • Integrates with LDAP, IAM, TCIM, TSM, SIEM, change management, CMDBs, etc. • Compliance workflow automation (electronic sign-offs, escalations) demonstrates oversight process • PCI Accelerator provides pre-configured reports based on best practices
11 Regularly test security systems and processes <ul style="list-style-type: none"> • Run internal and external vulnerability scans • Deploy integrity monitoring to detect modif. of critical sys. files 	Integrated vulnerability scanning, file integrity monitoring & behavioral vulnerability testing <ul style="list-style-type: none"> • Includes hundreds of pre-configured vulnerability tests for all major DBMS/OS combinations • Tracks changes to DB configuration files, environ./registry variables, executables and OS files
12 Maintain an Information Security Policy <ul style="list-style-type: none"> • Monitor/analyze alerts and distribute to appropriate personnel • Monitor and control all access to data 	Robust automated controls for enforcing information security policies <ul style="list-style-type: none"> • Real-time alerts, correlation alerts, centralized aggregation of all audit data, SIEM integration • Automated sign-offs demonstrate formal oversight process • 100% visibility & control over all database transactions (with blocking)

Gracias



Guardium[®]

SAFEGUARDING DATABASES™ AN IBM® COMPANY