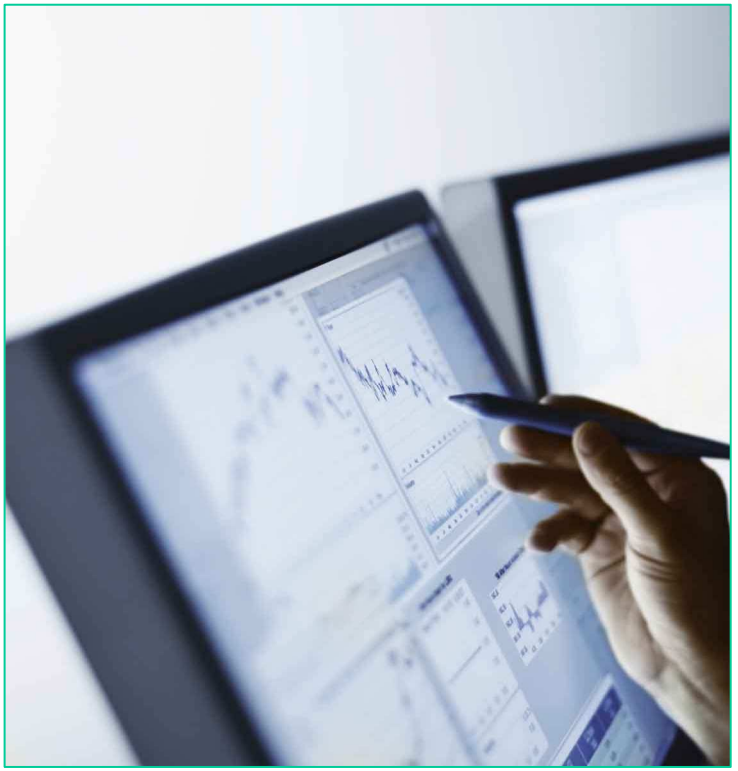
Auditoría, Monitorización y Protección de bases de datos: InfoSphere Guardium for z/OS V8R2 Guardium STAPs for z/OS (DB2, IMS, VSAM)

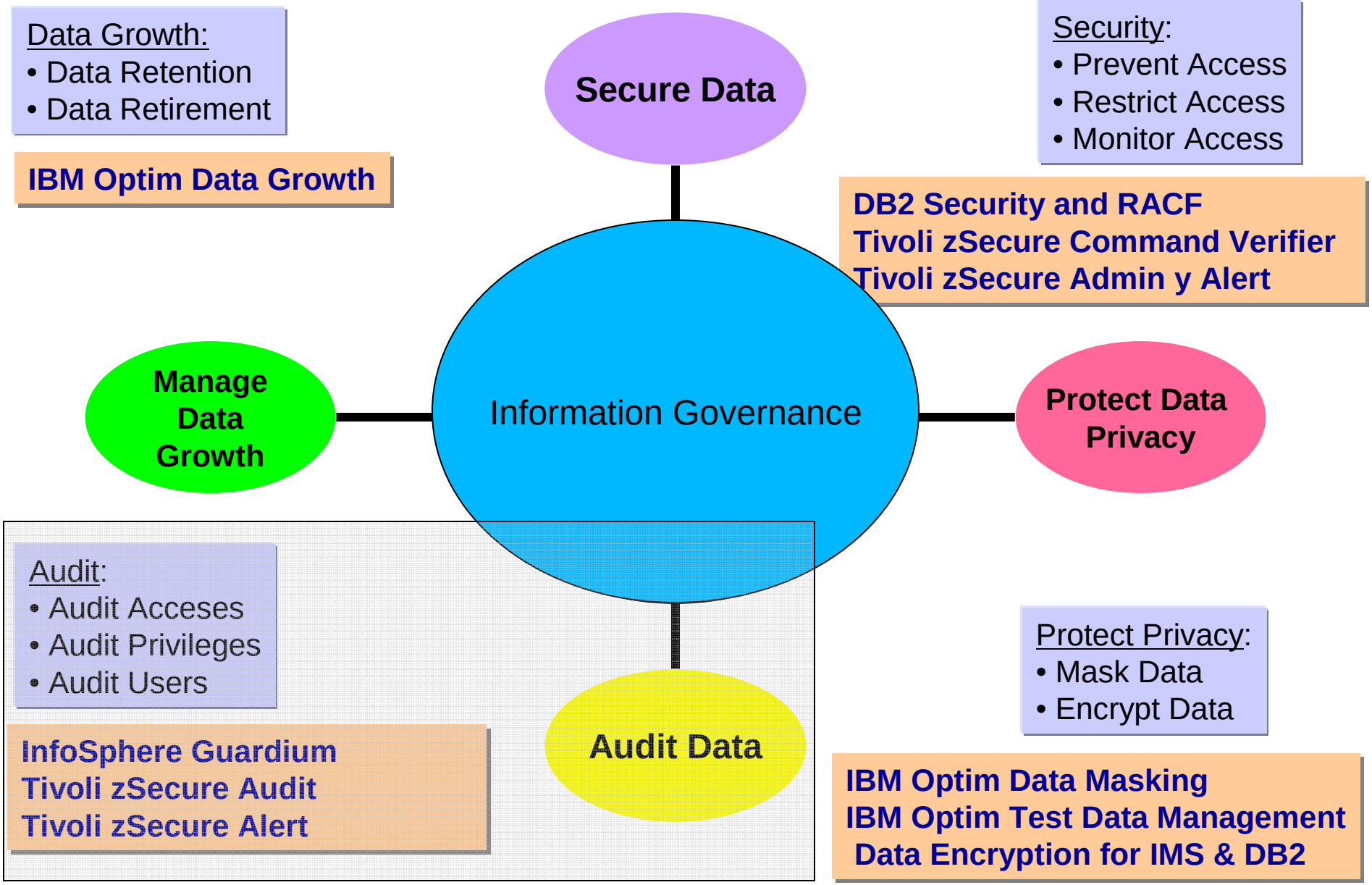
Sonia Márquez Paz – sonia_marquez@es.ibm.com

Agenda

- Introducción a InfoSphere Guardium
- Principales Novedades de InfoSphere Guardium V8.2 (comunes a las plataformas)
- InfoSphere Guardium V8.2 for DB2 z/OS
  - Novedades detalladas
  - Arquitectura V8.2
- InfoSphere Guardium V8.2 for VSAM
- InfoSphere Guardium V8.2 for IMS
- Resumen



Introducción a InfoSphere Guardium

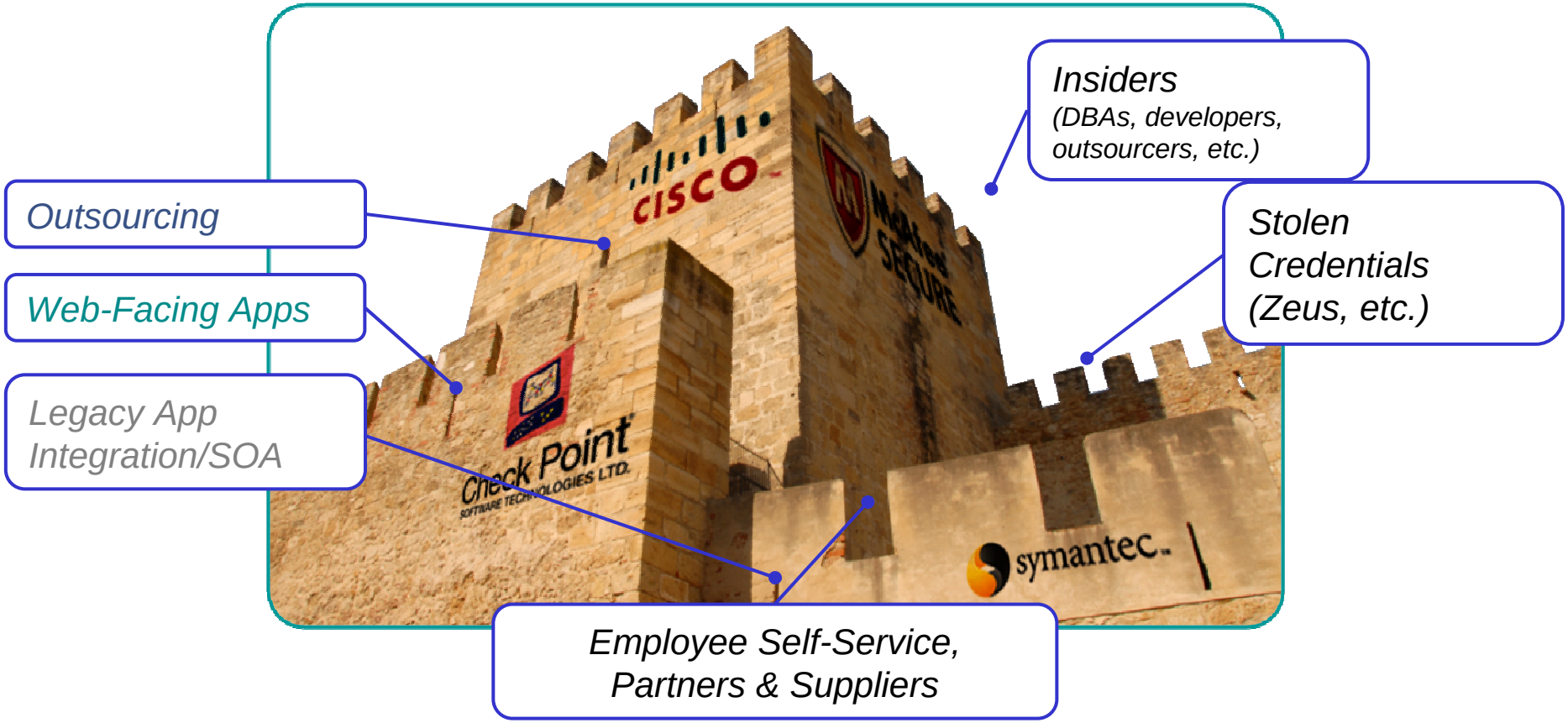


Problemática en el Negocio / Retos Habituales

Aumento de ataques y robos internos y externos de datos

Aumento del fraude por el robo de datos personales

Multas y sanciones por no cumplir normativa: SOX, PCI, LOPD, DP



InfoSphere Guardium permite a las empresas proteger su información más valiosa

Monitoriza continuamente el acceso a repositorios de datos de alto-valor para:

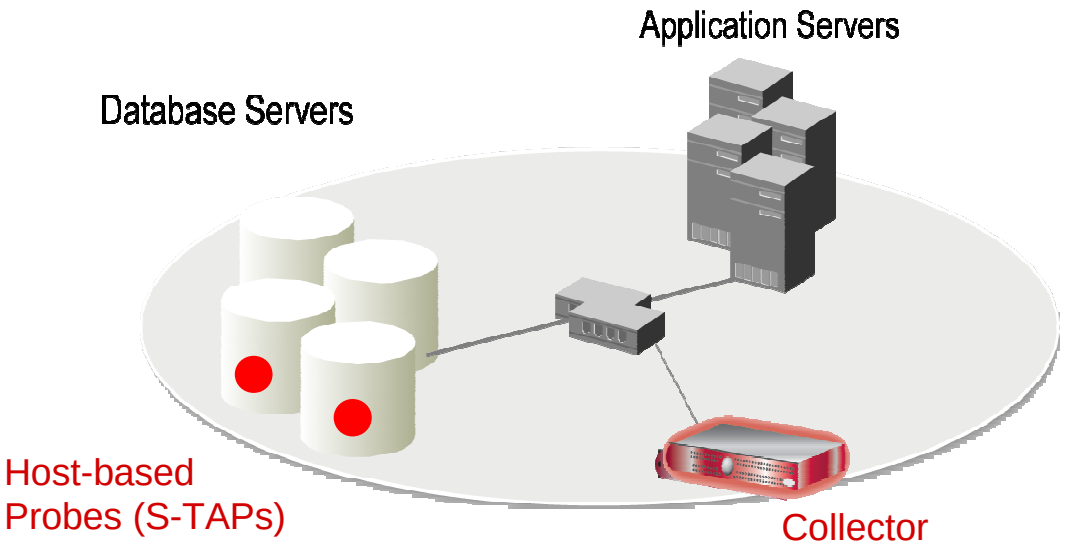
1. **Prevenir brechas de datos**
   Mitigar amenazas externas e internas

2. **Asegurar la integridad de datos sensibles**
   Previene contra cambios no autorizados sobre datos sensibles o estructuras

3. **Reducir el coste de cumplimiento con normativas y minimizar el riesgo de excepciones en auditorías**
   Automatizar y centralizar controles
   - Con SOX, PCI DSS, HIPAA/HITECH, FISMA…
   - En distintos gestores y aplicaciones

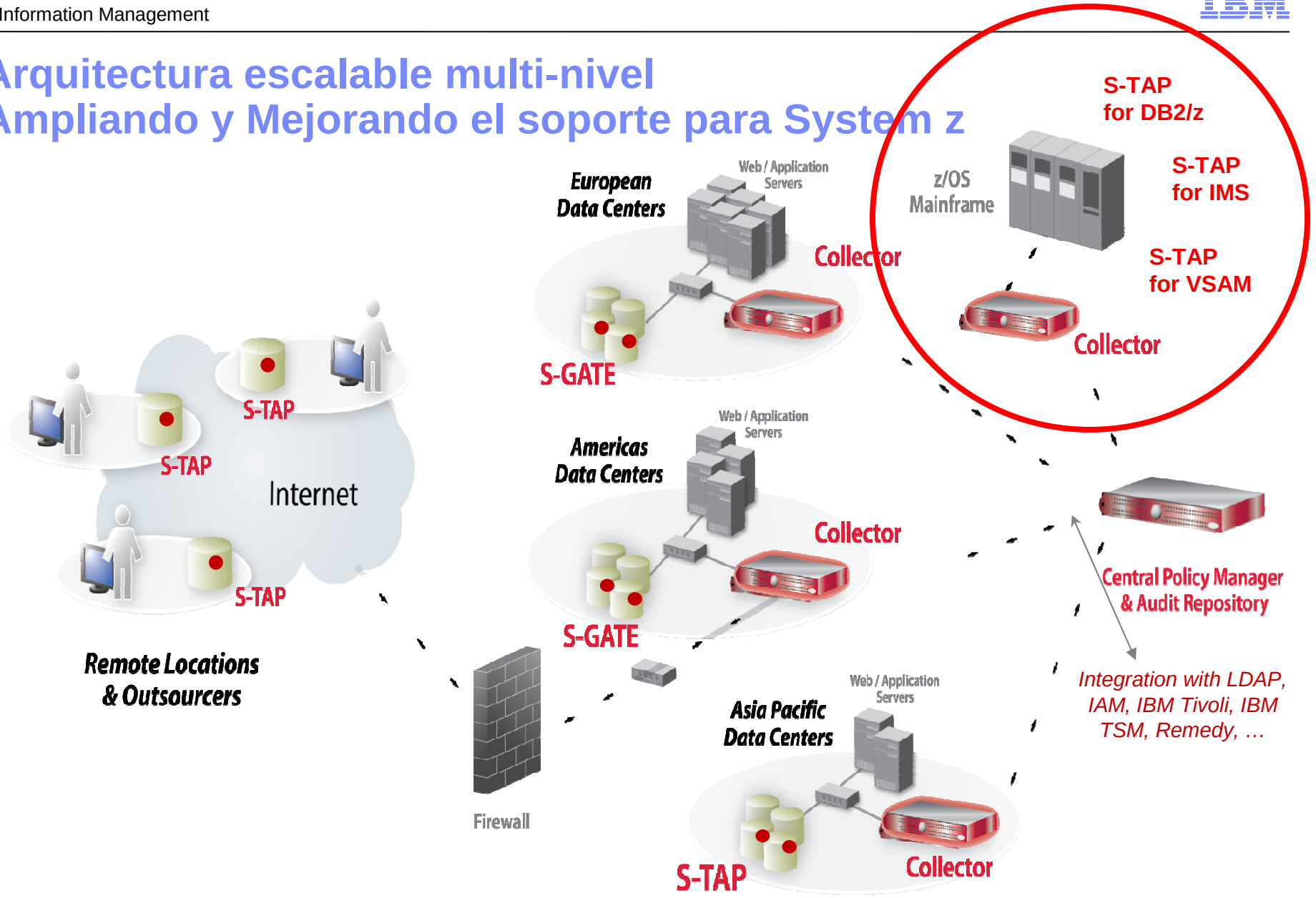
   Simplificar procesos

Monitorización, auditoría y protección en tiempo real con InfoSphere Guardium

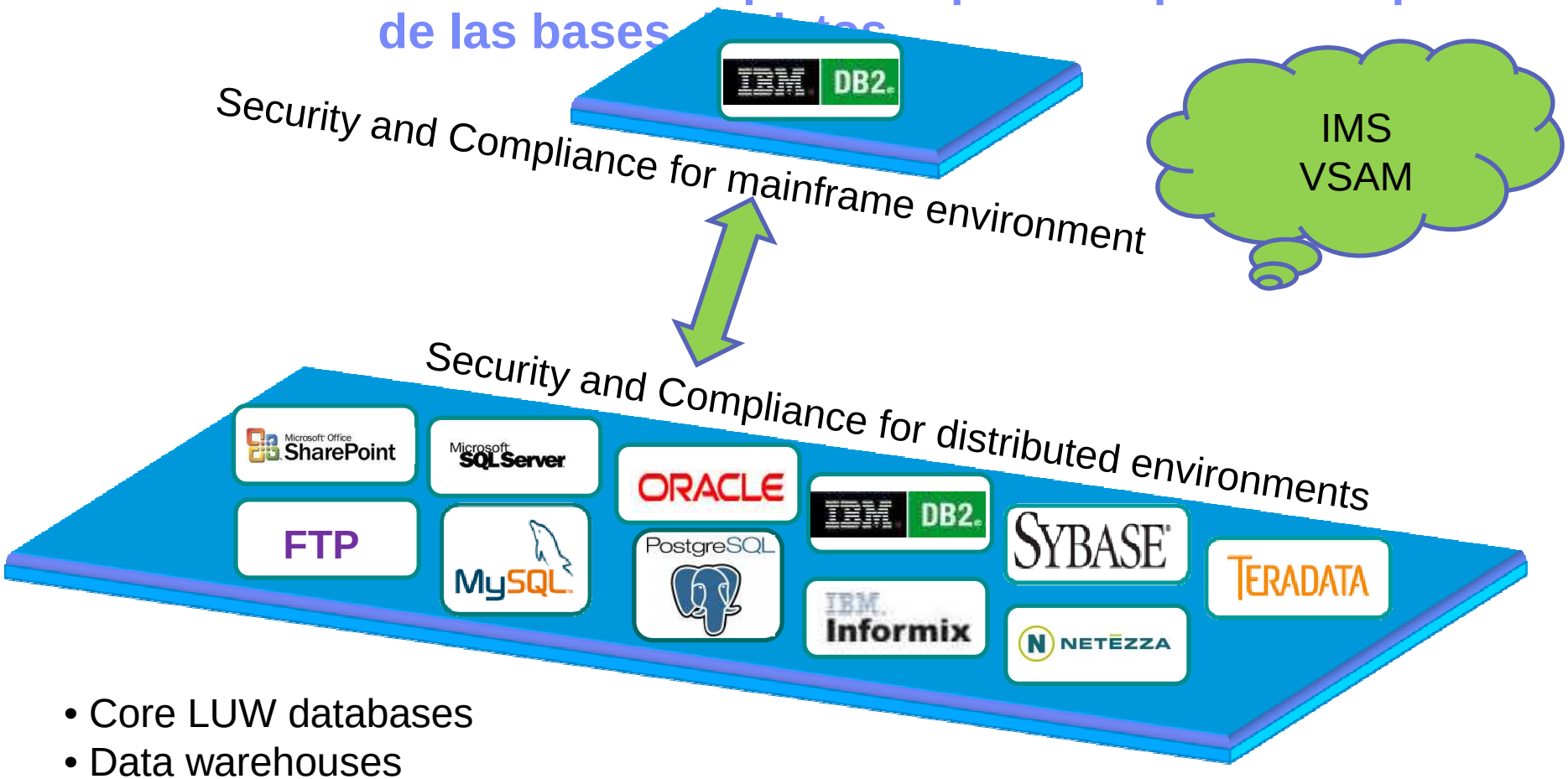


- **Sin cambios en gestores de bases de datos o aplicaciones**
- **No basado en logs del gestor, que pueden ser borrados por atacantes (internos o externos)**
- **100% visibilidad (accesos locales y remotos)**
- **Impacto mínimo en rendimiento**
- **Solución cross-DBMS (incluyendo z/OS)**
- **Granular, políticas en tiempo real y auditoría completa (q*uién, qué, cuándo, cómo)***
- **Informes automatizados de cumplimiento, gestión de firmas y escalados (regulaciones financieras, PCI DSS, privacidad de datos, etc.)**

Arquitectura escalable multi-nivel
Ampliando y Mejorando el soporte para System z

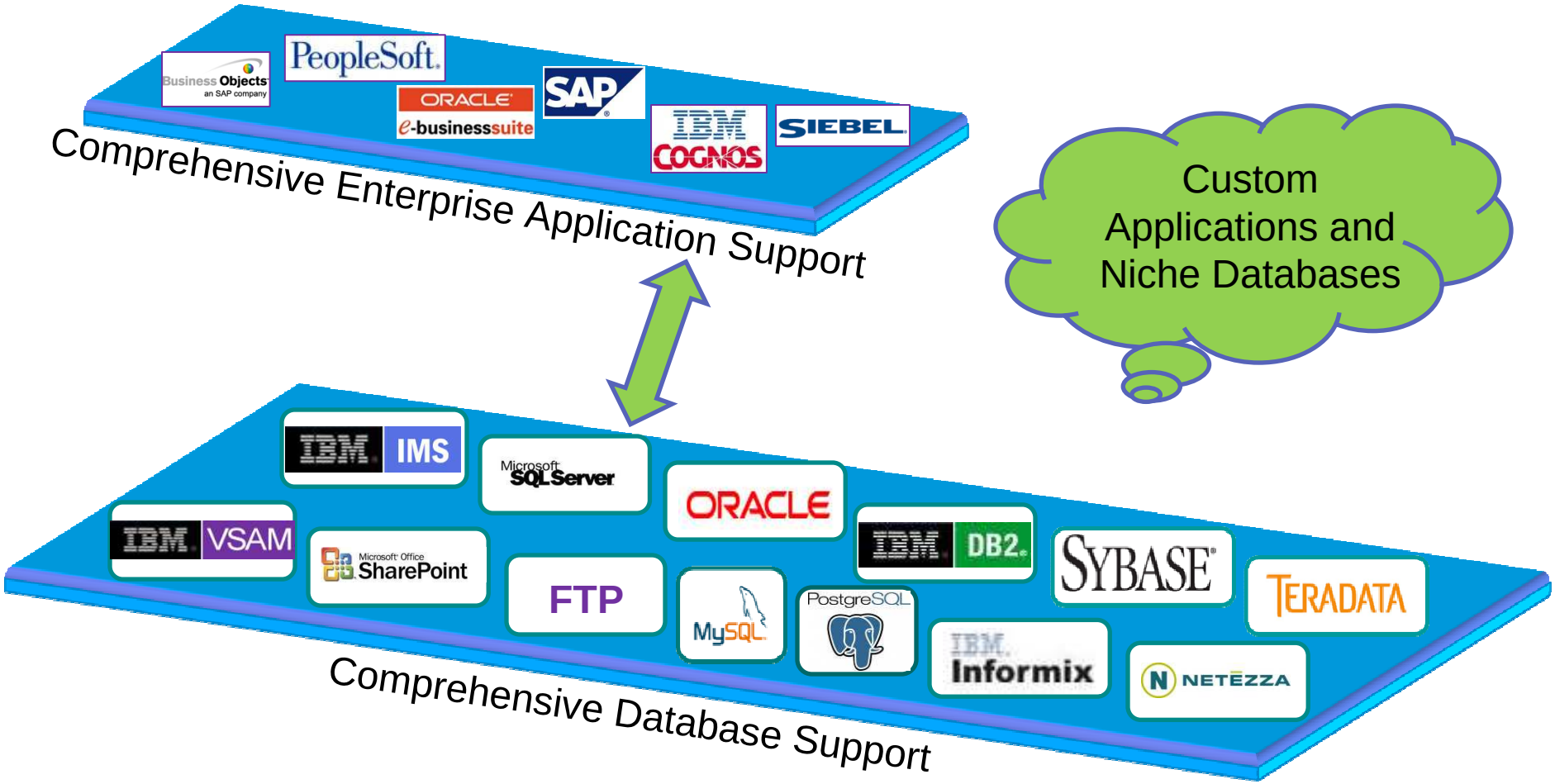


La seguridad y el cumplimiento a nivel global dentro de la empresa requiere soporte completo de las bases de datos

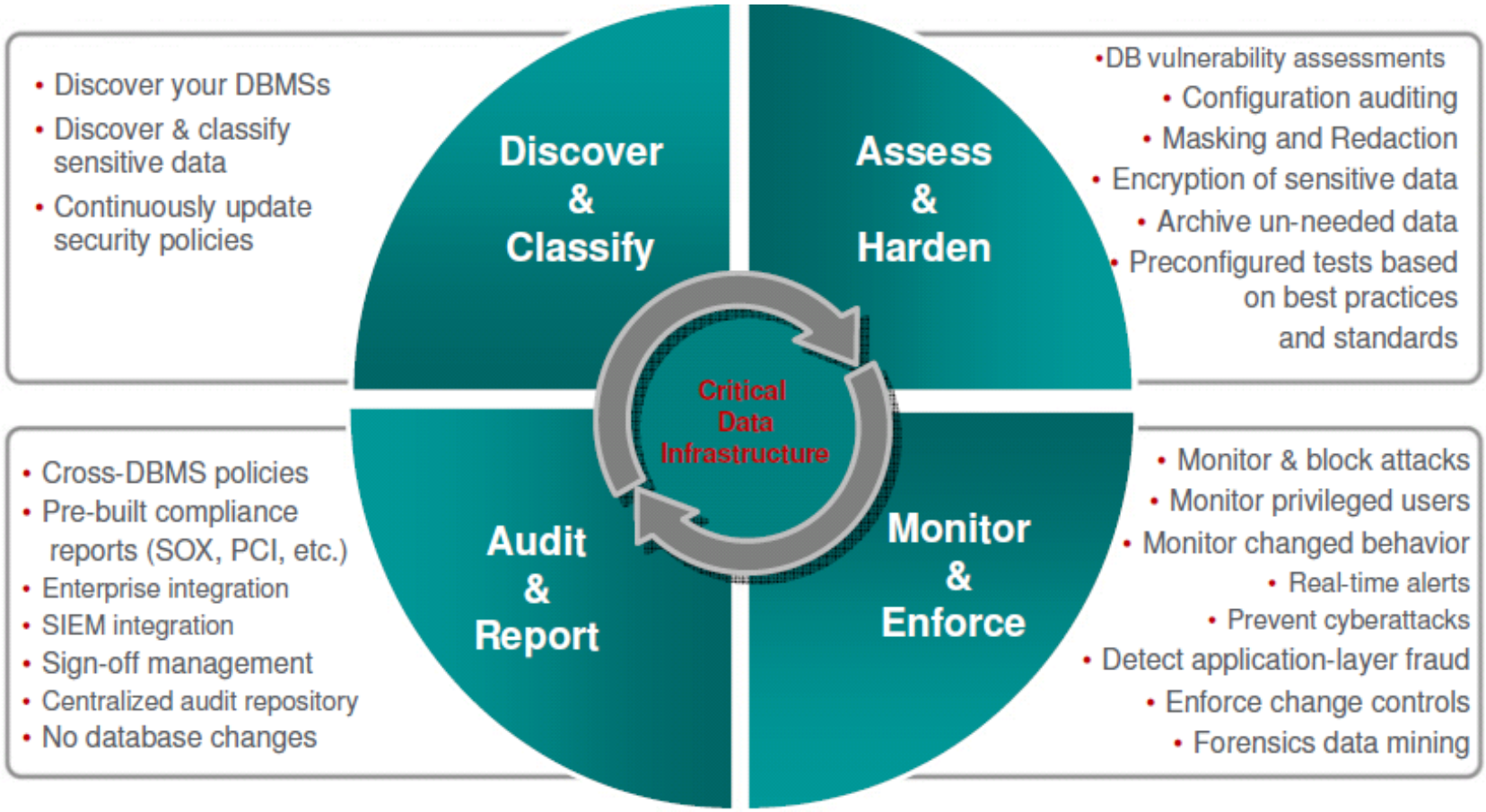


- Core LUW databases
- Data warehouses
- Open source LUW databases
- DB2 for z/OS
- File-based repositories

Soporte para aplicaciones de empresa

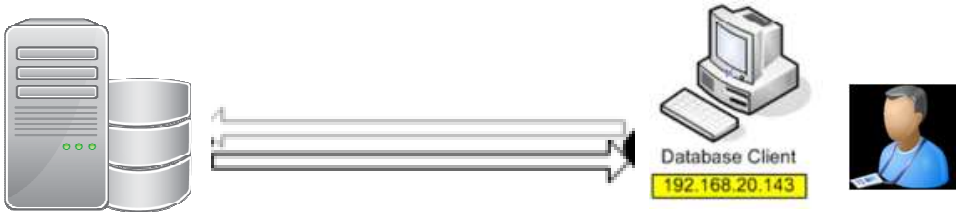


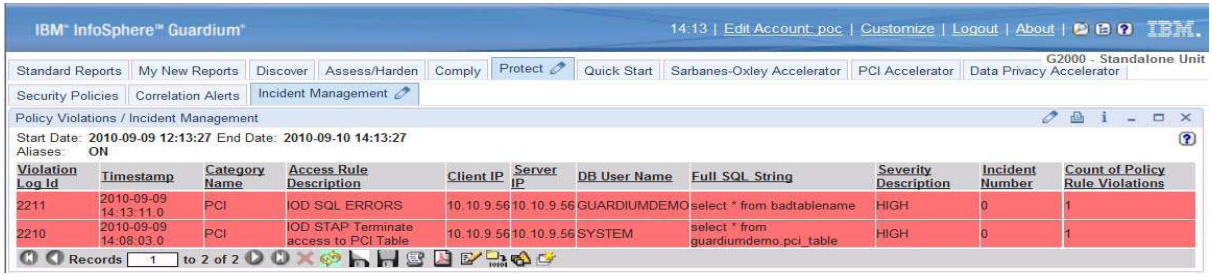
Gestión del ciclo de vida completo de la Seguridad en bases de datos y del Cumplimiento con Guardium

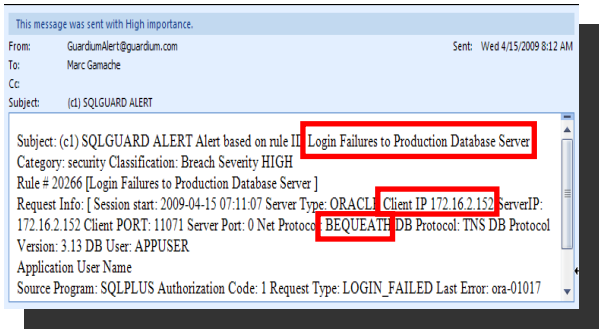


Monitorización y Reforzamiento de las Bases de Datos

- Tráfico local y remoto
- Log in y conexiones
- Actividad sobre bases de datos u objetos sensibles (DDLs, DMLs, DCLs)





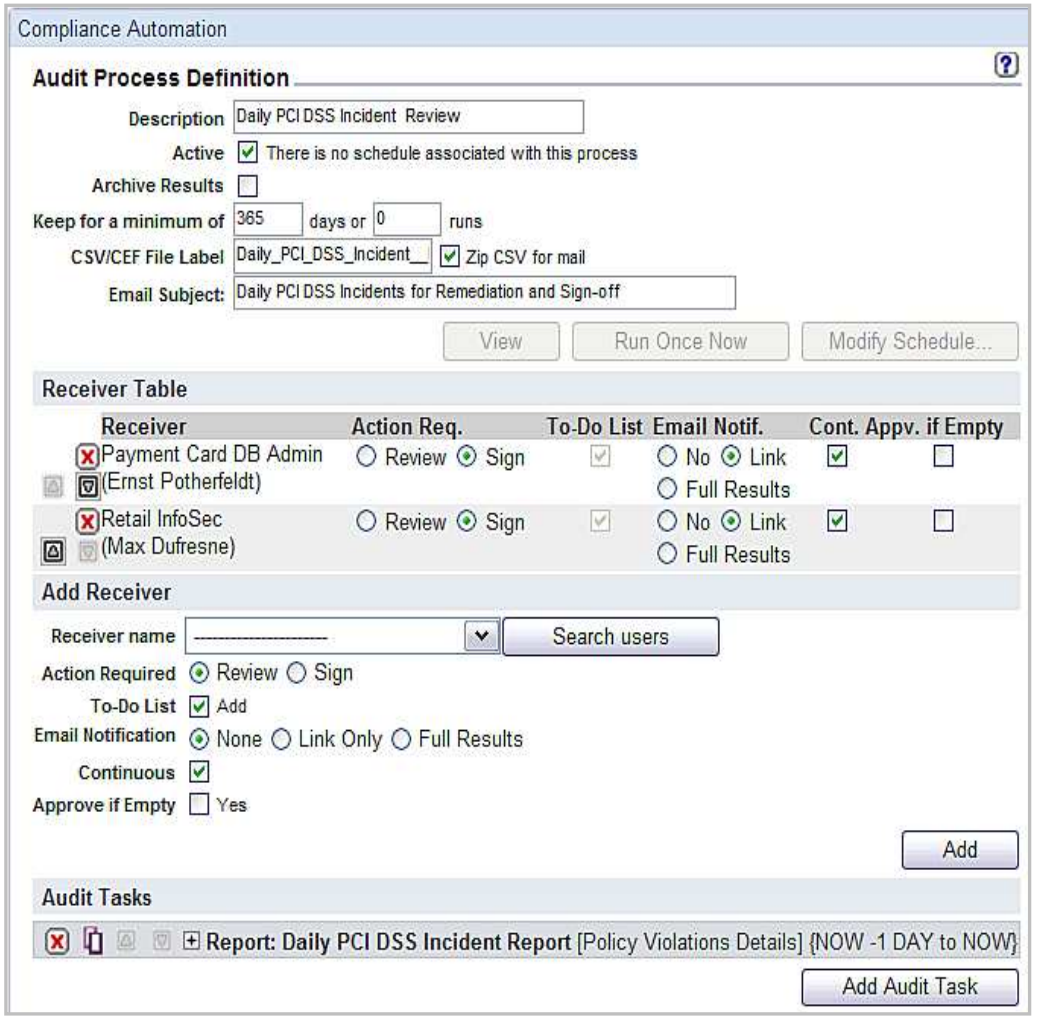


- Gestión de Incidencias
- Envío de Alertas y Bloqueos

Category Name	Access Rule Description	Client IP	Server IP	DB User Name
security	Login Failures to Production Database Server	10.10.9.56	10.10.9.56	APPUSER

Auditoría y Cumplimiento

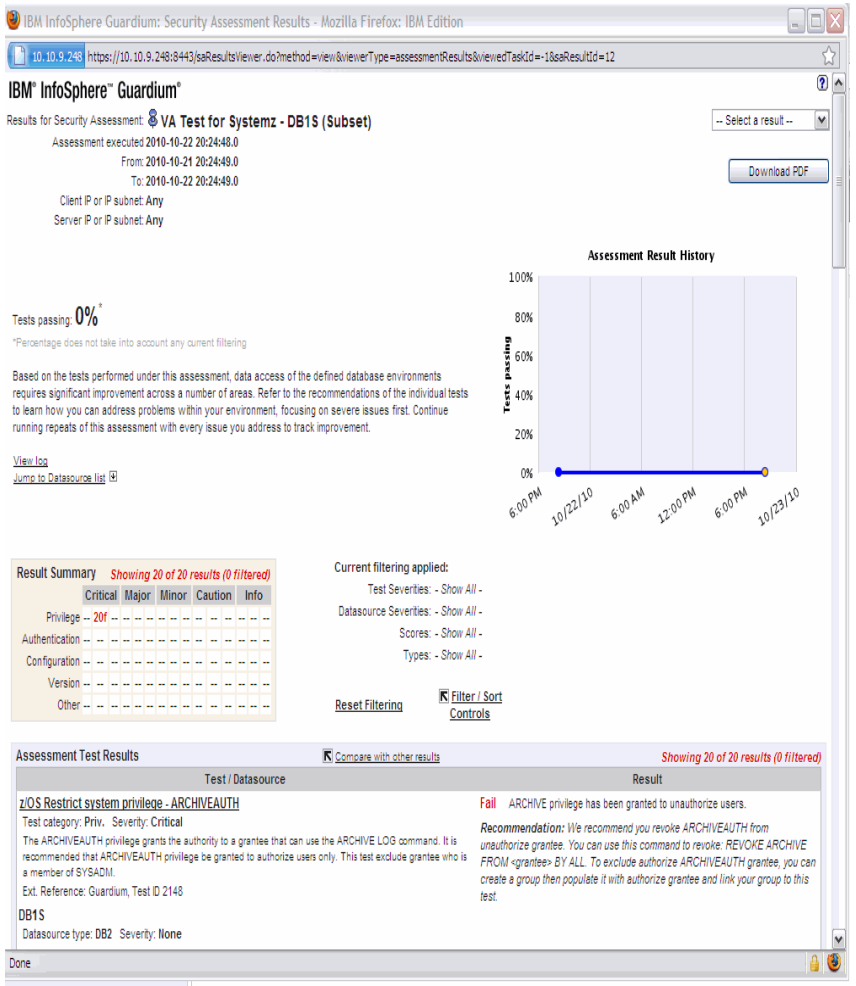
- Automatiza el proceso de Cumplimiento – Advanced Workflow
- Informes Predefinidos para el cumplimiento con políticas y regulaciones tales como PCI DSS, SOX, y directivas sobre Privacidad de Datos
- Capacidad de generar nuevos informes
- Evidencias para demostrar el cumplimiento con normativas
- Gestión de firmas (sign-off) y escalados



Automatización de proceso completo de auditoría evitando tareas manuales (más propensas a errores)

Análisis de Vulnerabilidades

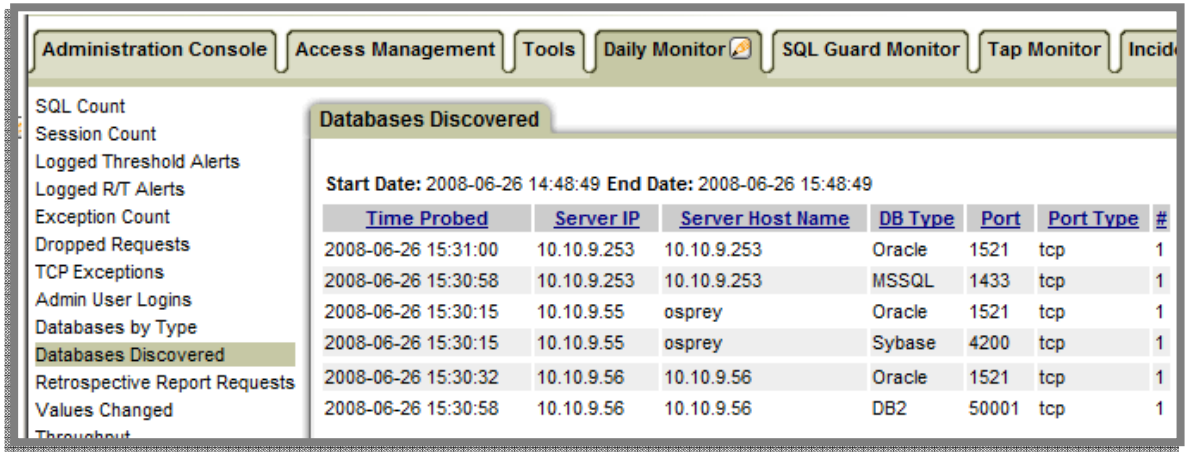
- Descubrir vulnerabilidades en Bases de Datos mediante tests predefinidos o configurables, basados en Best Practices de la Industria (STIG, CIS, CVE…)
- Actualizaciones periódicas para evitar amenazas
- Realizar chequeos de vulnerabilidad regularmente
- Identificar riesgos: parches no aplicados y críticos, privilegios mal configurados, passwords débiles, cuentas por defecto, etc



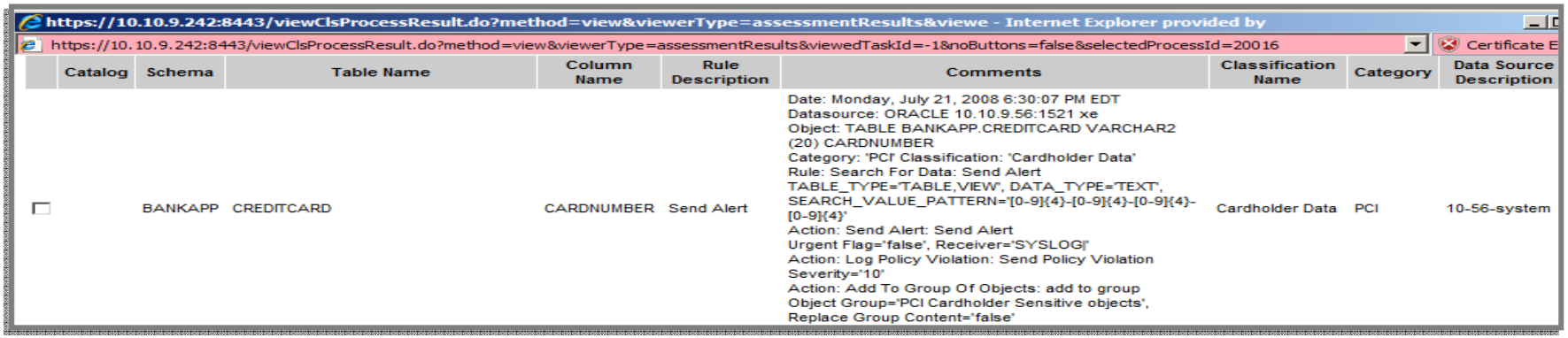
Los Auditores necesitan evidencias de controles, procesos y procedimientos adecuados

Descubrimiento y Clasificación de Información Sensible

Descubrimiento de Bases de Datos

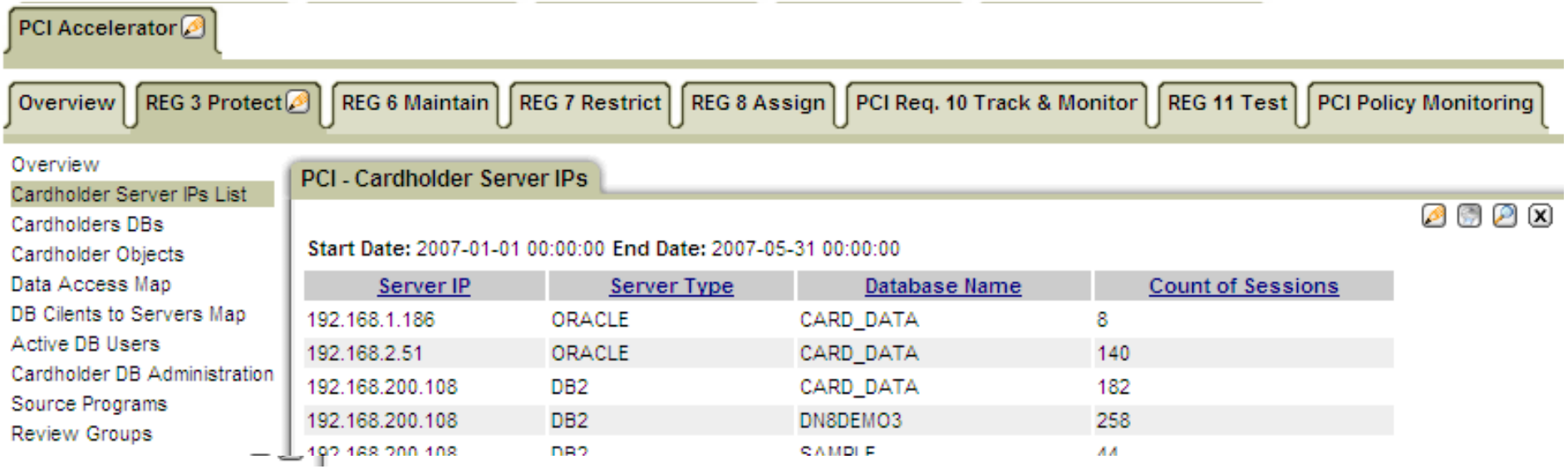


Descubrimiento y Clasificación de Información Sensible



Auditoría y Generación de Informes (Reporting)

- **Dispone de diversos aceleradores de cumplimiento de normativas (SOX, PCI, Privacidad de Datos…)**
  - 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.)



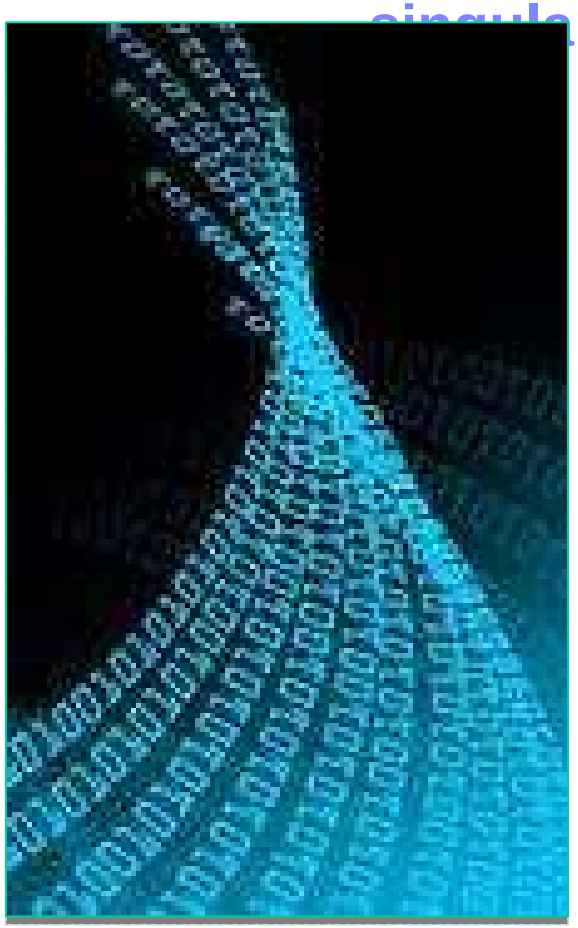
Monitorización mejorada de SAP para detectar Fraude

Application Type	User	Item Name	Operation Type	Transaction Code
SAP	HANSSCHMIDT	HFPT_COEJA_PP_ORDER_RPSCO_V2	Query	Change Order (IW32)
SAP	HANSSCHMIDT	MATERIAL	Update	Create Material (MMZ1)
SAP	VOLKERHIESTERMANN	BANK	Update	Change Bank (FI02)
SAP	HANSSCHMIDT	ADRESSE3	Update	User Maintenance (SU01)
SAP	GEORGHELD	ADRESSE3	Update	User Maintenance (SU01)
SAP	GEORGHELD	ADRESSE3	Update	User Maintenance (SU01)
SAP	HANSSCHMIDT	MATERIAL	Update	Create Material (MMZ1)
SAP	HANSSCHMIDT	MATERIAL	Update	Change Material (MMZ2)
SAP	HANSSCHMIDT	ORDER	Update	Change Order (IW32)

- Información detallada de los usuarios de SAP
  - *Va más allá de lo que muestran los logs de transacciones*
- Detección de fraude y otras actividades no autorizadas
- No se necesitan cambios en la aplicación o la base de datos
- Disponible para Oracle y DB2

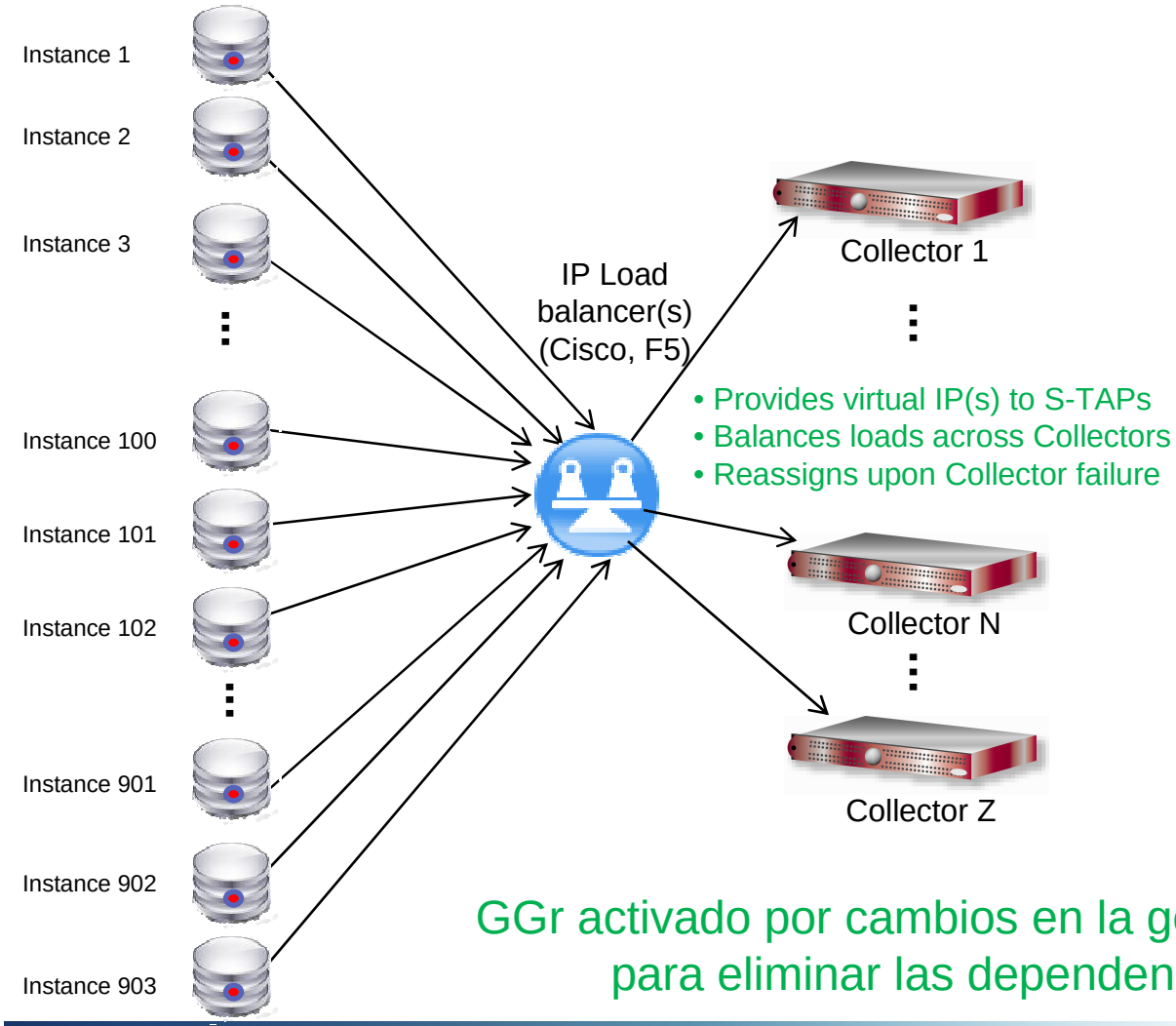
Novedades InfoSphere Guardium 8.2 (comunes)

Con el nuevo Universal Feed, el sistema InfoSphere Guardium se abre, permitiendo que todas sus capacidades se puedan aplicar a aplicaciones de cliente y bases de datos singulares



- **El protocolo InfoSphere Guardium (agente a Colector) se hace disponible a clientes y otras empresas**
  - Proporciona un medio de soporte para segmentos fragmentados de mercado: aplicaciones a medida, bases de datos nicho, etc.
  - Modelo de auditoría de datos; no es un SIEM
- **El cliente/partner es responsable de desarrollar el interfaz para integrar el sistema (p.ej. el equivalente al S-TAP)**
  - Se usa un protocolo estándar Open Industry para simplificar el desarrollo
- **Soporte de capacidades completas, o bien de un subconjunto de las capacidades de InfoSphere Guardium**
  - Monitorización y protección
  - Tiempo-Real
  - Registro de auditoría seguro, automatización del workflow de compliance, etc.

El nuevo InfoSphere Guardium Grid (GGr) mejora la flexibilidad a la vez que reduce los costes operacionales



Beneficios:

- Con una VIP se simplifica la configuración del S-TAP, reduciendo los costes de despliegue
- El sistema asigna el colector apropiado para nuevos S-TAPs basados en la disponibilidad y capacidad, reduciendo los costes de planificación
- Los colectores se pueden añadir (o eliminar) según crece el sistema sin modificar las configuraciones, reduciendo los costes operacionales
- Preserva las características de redundancia completa y balanceo de carga del sistema

GGr activado por cambios en la gestión central para eliminar las dependencias IP

Sensitive Data Finder: mejoras en matching y rendimiento, con nuevo soporte de automatización

Sensitive Data Finder Overview

• Automatiza el proceso de búsqueda y clasificación de datos sensibles
• Soporta múltiples acciones de respuesta: generación de alertas en tiempo real, aplicación automatizada de políticas apropiadas, etc.
• Cuatro técnicas de búsqueda complementarias para maximizar la identificación
• Integrado con workflow y otras aplicaciones para minimizar los costes operacionales

- **Capacidad ampliada para buscar patrones de datos o valores**
  - Se añade soporte para algoritmos a medida al soporte regex previo (p. ej. DNI, NIF)
  - Clase Java conforme al interfaz IBM
- **Soporte para agrupación de reglas**
  - Deben cumplirse los requisitos de todas las reglas del grupo, para que se dé un “match”
  - Ejemplo: número de tarjeta de crédito y código de verificación, etc.
- **Se añaden umbrales de “match”**
  - Lleva un registro del número de “matches” y los compara a los umbrales definidos por el usuario
  - Reduce los falsos positivos
- **Muestreo consolidado para mejorar el rendimiento**
- **Soporte API para permitir la automatización basada en script**
- Resultado: Mejoras en **rendimiento y descubrimiento**

InfoSphere Guardium Supported Platforms	Supported Versions
Oracle	8i, 9i, 10g (r1, r2), 11g, 11gr2
Oracle (ASO, SSL)	9i, 10g(r1,r2), 11g
Microsoft SQL Server	2000, 2005, 2008
Microsoft SharePoint	2007, 2010
IBM DB2 (Linux, Unix, Linux for System z)	9.1, 9.5, 9.7
IBM DB2 (Windows)	9.1, 9.2, 9.5, 9.7
IBM DB2 for z/OS	8.1, 9.1, 10.1
IBM DB2 for iSeries	V5R2, V5R3, V5R4, V6R1
IBM IMS	9, 10, 11, 12
IBM Informix	7, 9, 10,11, 11.5, 11.7
MySQL and MySQL Cluster	4.1, 5.0, 5.1
Sybase ASE	12, 15, 15.5
Sybase IQ	12.6, 12.7, 15
Netezza	NPS 4.5, 4.6, 4.6.8, 5.0, 6.0
PostgreSQL	8,9
Teradata	6.X, 12, 13, 13.1
FTP	

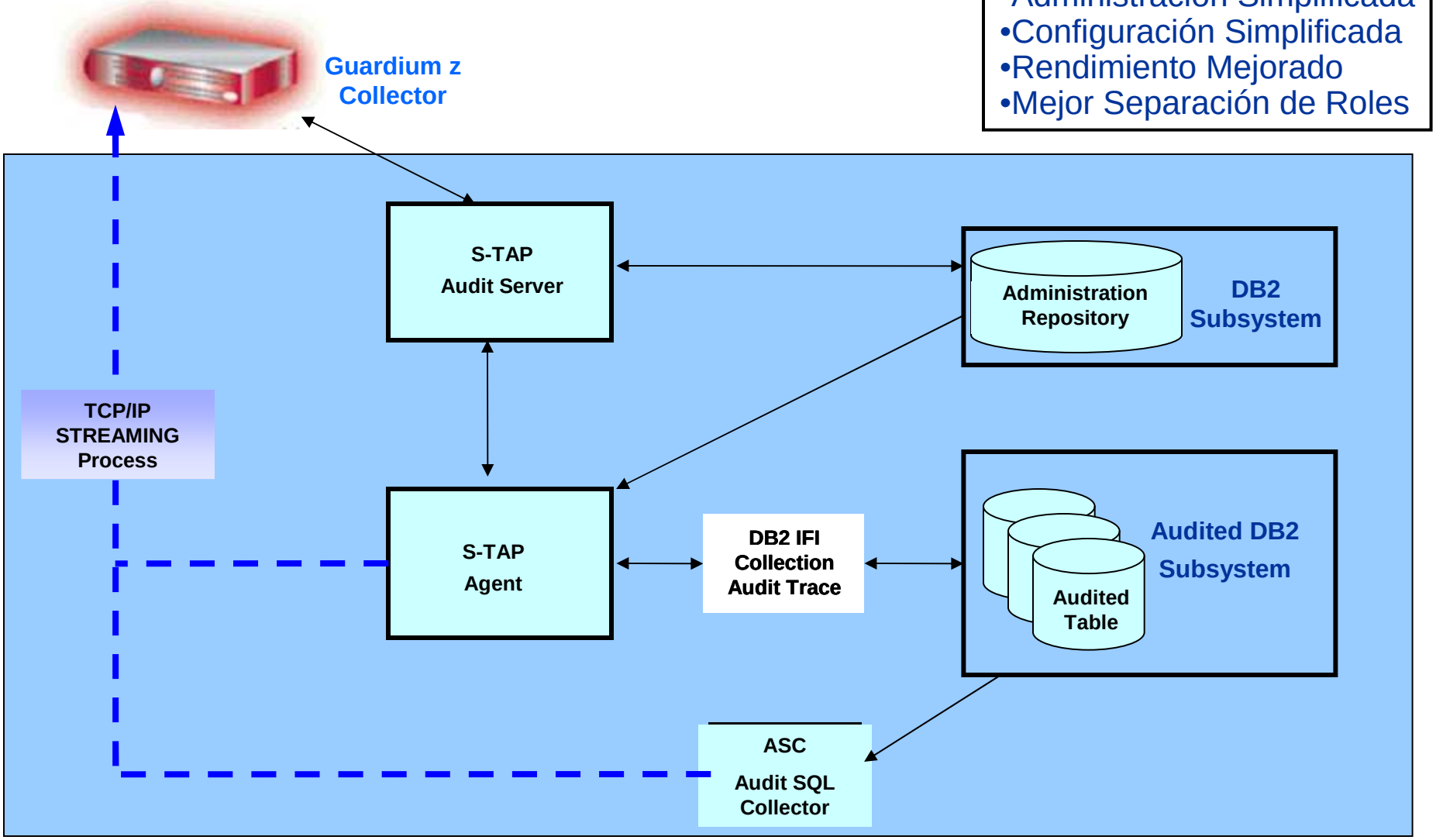
Novedades Guardium 8.2 for DB2 z/OS

IBM InfoSphere Guardium S-TAP for DB2 on z/OS 8.1

- No hay cambio en la versión del S-TAP for DB2 on z/OS 8.2…sino que se distribuyen los cambios mediante PTFs sobre la release 8.1
- **Mejoras implantadas desde Diciembre de 2010**
  - Nuevo filtrado por CONNECTION TYPE, PROGRAM, NEW SQLID y original AUTHID
  - Mejoras en el proceso general de Filtrado
  - Reducción en el uso de CPU durante procesado de eventos IFI
  - Mejoras en el streaming de Datos de Audit al appliance
  - Descarga de actividad a procesadores zIIP
- **Mejoras añadidas para la release 8.2**
  - Soporte de 'policy push down'
  - Streaming para datos IFI (eliminación de ficheros de offload y FTP)
  - Informe sobre errores y problemas de STAP al Appliance Guardium
  - Auditoría de eventos de DDL (Create/Alter/Drop) en tarea ASC
  - Stage 0 Filtering

Guardium S-TAP for DB2 on z/OS Arquitectura Release 8.2

- Administración Simplificada
- Configuración Simplificada
- Rendimiento Mejorado
- Mejor Separación de Roles



Guardium for DB2 on z/OS Novedades V8.2

En 8.2:

Rendimiento Mejorado

Menor overhead del S-TAP

Nuevos campos para filtrado – ej. filtrado por attach

Administración Simplificada – se integra la administración del S-TAP dentro del interfaz del appliance

Despliegue Simplificado – se elimina el FTP – todos los datos de auditoría se transmiten al appliance por streaming

Diagnóstico mejorado – Nueva información de estado enviada al appliance

Vulnerability Assessments más completos para DB2/z

Guardium for DB2 on z/OS Novedades V8.2

Otras mejoras

- **Auditoría de DDL** (create/alter/drop) sin añadir audit flag a las tablas
- Recogida de eventos DDL Create/Alter/Drop cambia de IFI (trazas) **al ASC**
- Captura **todo el DDL** y de **más tipos de objetos** – no sólo el proporcionado por trazas en una tabla
- **Rendimiento Mejorado** - Filtrado Stage 0 por plan y tipo de conexión
- **Uso adicional de zIIPs**
- **Cifrado SSL entre el S-TAP y el appliance**
- **Entitlement Reporting para DB2/z**

Soporte adicional para filtrado de eventos

- **Connection Type:** Filtrado sobre uno o más tipos de los siguientes:

  1. TSO => TSO FOREGROUND AND BACKGROUND
  2. CALL => DB2 CALL ATTACH
  3. BATCH => DL/I BATCH
  4. CICS => CICS ATTACH
  5. BMP => IMS ATTACH BMP
  6. MPP => IMS ATTACH MPP
  7. PRIV => DB2 PRIVATE PROTOCOL
  8. DRDA => DRDA PROTOCOL
  9. CTL => IMS CONTROL REGION
  10. TRAN => IMS TRANSACTION BMP
  11. UTIL => DB2 UTILITIES
  12. RRSAF => RRSAF

- **Original Authorization ID**
- **Program Name**
  - Suele ser típicamente el DB2 package name
  - Útil cuando se requiere auditar sólo unos pocos paquetes en un plan multi-package

Vulnerability Assessment Tests en Guardium DB2 z/OS V8.2

- Nueva capacidad que permite a las empresas mejorar significativamente la seguridad de sus entornos mainframe, realizando pruebas de análisis de vulnerabilidades en bases de datos de manera automatizada
  - Test preparados para detectar vulnerabilidades, incluyendo privilegios inapropiados, grants, cuentas por defecto, etc.
  - Capacidades que permiten el desarrollo de pruebas a medida
- **Basados en los estándares de seguridad del grupo de Desarrollo del DB2 en Silicon Valley Lab, y estándares de la industria como DISA STIG y CIS**
  - Server defaults
  - Patch levels
  - OS and DBMS Vulnerability Assessment
- Se añaden nuevas consultas al catálogo para detectar riesgos potenciales
- Se verifican también parámetros de seguridad del subsistema DB2 (DSNZPARM)
- Existen tests para buscar “huérfanos” z/OS
  - Los huérfanos son authorization IDs con privilegios, que no aparecen en la base de datos de RACF
- “Patch” Tests para PTFs relacionadas con Seguridad
  - Más de 40 tests sobre APARes inicialmente
  - Se proporcionan actualizaciones trimestrales
- Funcionalidad Exclusiva de IBM

System Z Vulnerability Assessment

IBM® InfoSphere™ Guardium®

Results for Security Assessment: **VA test for system Z**
Assessment executed **2010-09-20 13:55:27.0**
From: **2010-09-19 13:55:27.0**
To: **2010-09-20 13:55:27.0**
Client IP or IP subnet: **Any**
Server IP or IP subnet: **Any**

Tests passing: **88%***

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 73 of 73 results (0 filtered)

	Critical	Major	Minor	Caution	Info
Privilege	46p 4f	7p 1f	–	–	–
Authentication	–	–	–	–	–
Configuration	1p	–	–	–	–
Version	–	1p	–	–	–
Other	1p	3p 2f	2p 1f	–	3p 1f

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

Assessment Test Results

Test / Datasource

z/OS Grant option - Resauth
Test category: **Priv.** Severity: **Critical**
This test check for privileges on various resources that has been granted with the grant option. These resource include: Buffer pool, Collection, Distinct type, Table space, Storage group and JAR file. Grant option is not a good practice and should be avoid where possible. When privileges are granted with the grant option, a user can grant privileges on that resource to other users. We do not recommend granting resource privilege with grant option. This test exclude grantee who is a member of SYSADM and SYSIBM user.
Ext. Reference: Guardium, Test ID 2179

System Z Datasource
Datasource type: **DB2** Severity: **None**

Details: Grantee causing failure: Grantee=ADMIN_A: Obtype=D: Qualifier=GU0003: Name=CANADIAN_DOLLAR
Grantee=ADMIN_A: Obtype=D: Qualifier=GU0002: Name=CANADIAN_DOLLAR

Fail — One or more resources privileges has be

Recommendation: We recommend that you rev
resource privilege so that you are using grant inst
must have grant option, you can create a group t
group to this test.

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

Fail — One or more object privileges has been

Recommendation: We recommend that you rev
schema privilege so that you are using grant inst
have grant option, you can create a group then p
this test.

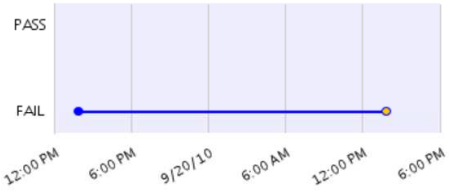
IBM InfoSphere Guardium: Security Assessment Results - Mozilla Firefox

9.70.147.47 https://9.70.147.47:8443/saResultsViewer.do?method=view&viewerType=testResultDetails&viewedTaskId=-1&selectedTestResultId=20158&saResultId=20001

IBM® InfoSphere™ Guardium®

Results for Security Assessment: **VA test for system Z**
Assessment executed **2010-09-20 13:55:27.0**
From: **2010-09-19 13:55:27.0**
To: **2010-09-20 13:55:27.0**
Client IP or IP subnet: **Any**
Server IP or IP subnet: **Any**

Test Result History



z/OS Grant option - Resauth
Test category: **Priv.** Test severity: **Critical**

System Z Datasource
Datasource type: **DB2** Datasource severity: **None**

Fail

One or more resources privileges has been granted with the grant option.

Short Description: This test check for privileges on various resources that has been granted with the grant option. These resource include: Buffer pool, Collection, Distinct type, Table space, Storage group and JAR file. Grant option is not a good practice and should be avoid where possible. When privileges are granted with the grant option, a user can grant privileges on that resource to other users. We do not recommend granting resource privilege with grant option. This test exclude grantee who is a member of SYSADM and SYSIBM user.

External Reference: Guardium, Test ID 2179

Recommendation: *We recommend that you revoke resources privileges granted with the grant option. Please redo your resource privilege so that you are using grant instead of grant option. If you need to exclude certain grantee or resource that must have grant option, you can create a group then populate it with authorize grantee and or resource name and link your group to this test.*

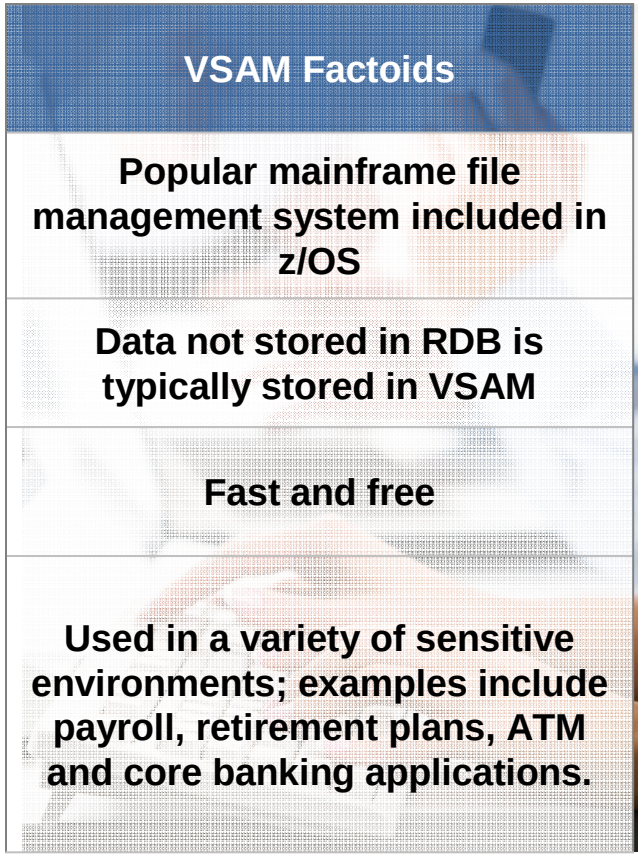
Details: Grantee causing failure: Grantee=ADMIN_A: Obtype=D: Qualifier=GU0003: Name=CANADIAN_DOLLAR
Grantee=ADMIN_A: Obtype=D: Qualifier=GU0002: Name=CANADIAN_DOLLAR

Close this window

Done

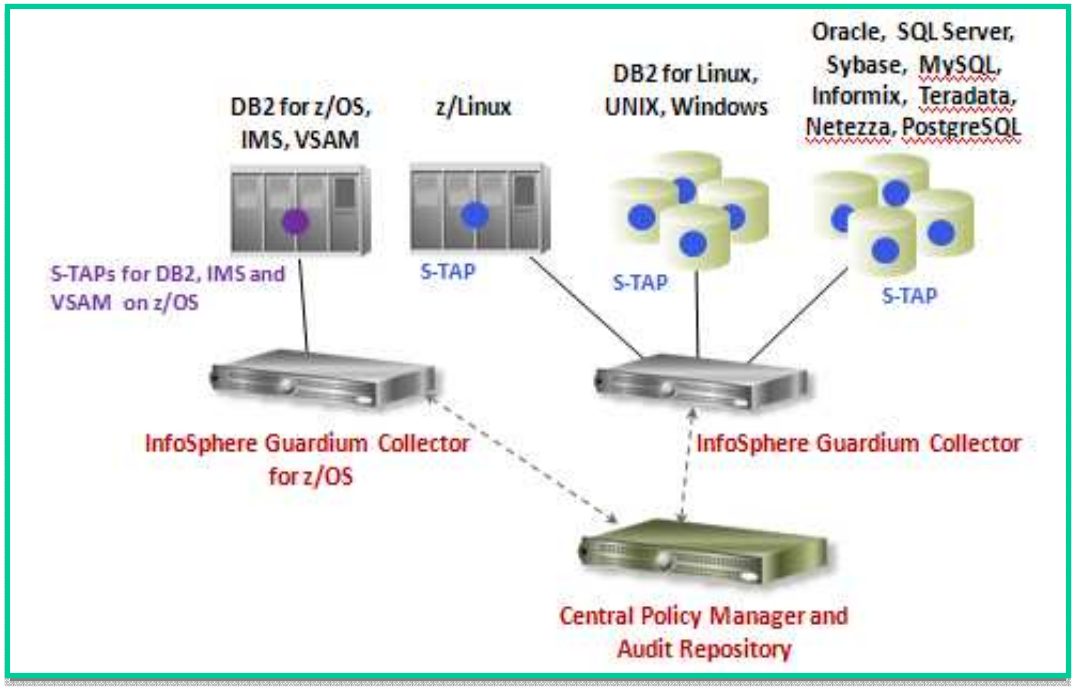
Guardium STAP for VSAM on z/OS 8.2

El VSAM es importante desde el punto de vista de seguridad y cumplimiento



- Constituye el repositorio para muchas aplicaciones que manejan datos sensibles
- Es el repositorio que soporta muchas aplicaciones críticas de las empresas
- Aumento en las exigencias de las auditorías que afectan a datos en VSAM
- Las empresas tienen los mismos requisitos para sus entornos VSAM que para otros tipos de gestores de bases de datos
- No resulta práctico disponer de soluciones de auditoría y seguridad diferentes para distintos entornos

Nuevo S-TAP for VSAM

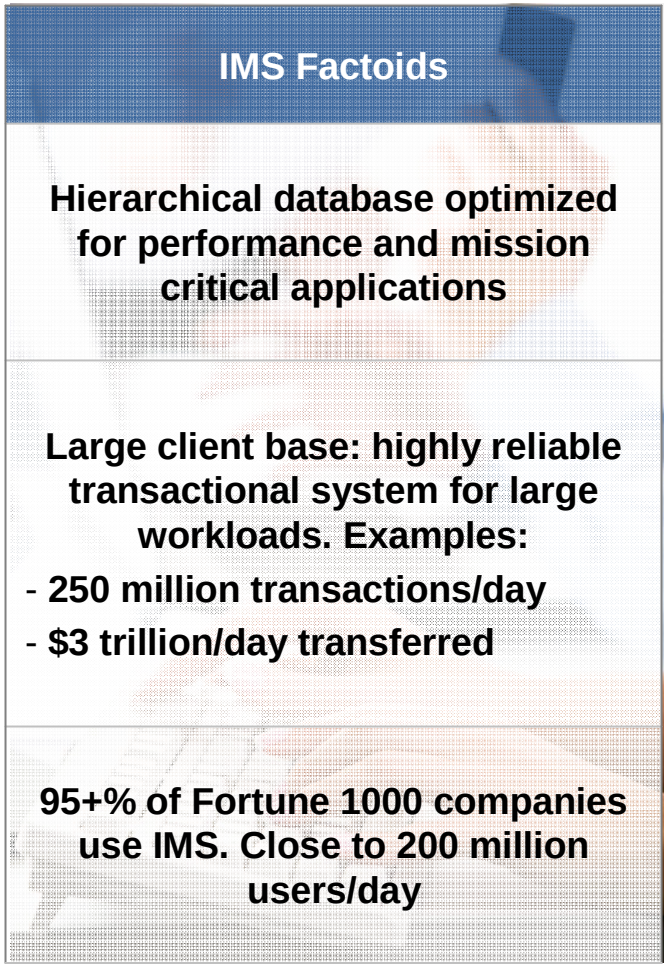


- **Nuevo agente que aprovecha la tecnología existente de IBM para captura de eventos**
- **Soporta ficheros de tipo ESDS, KSDS, RRDS, VRRDS y LDS**
- **Captura en tiempo real de eventos VSAM**
  - Data set OPENs, UPDATEs, DELETEs, RENAMEs, CREATEs, ALTERs,
  - RACF ALTERs, CONTROLs, UPDATEs, READs
- **El colector proporciona funcionalidad consistente con otros agentes**
  - Registro de auditoría seguro
  - Reporting
  - Detección de violaciones de políticas
  - Workflow de Compliance, etc.
- **Auditoría para utilidades fuera de DB2**

Plus significant enhancements to the performance and manageability of the existing S-TAP for DB2 on z/OS

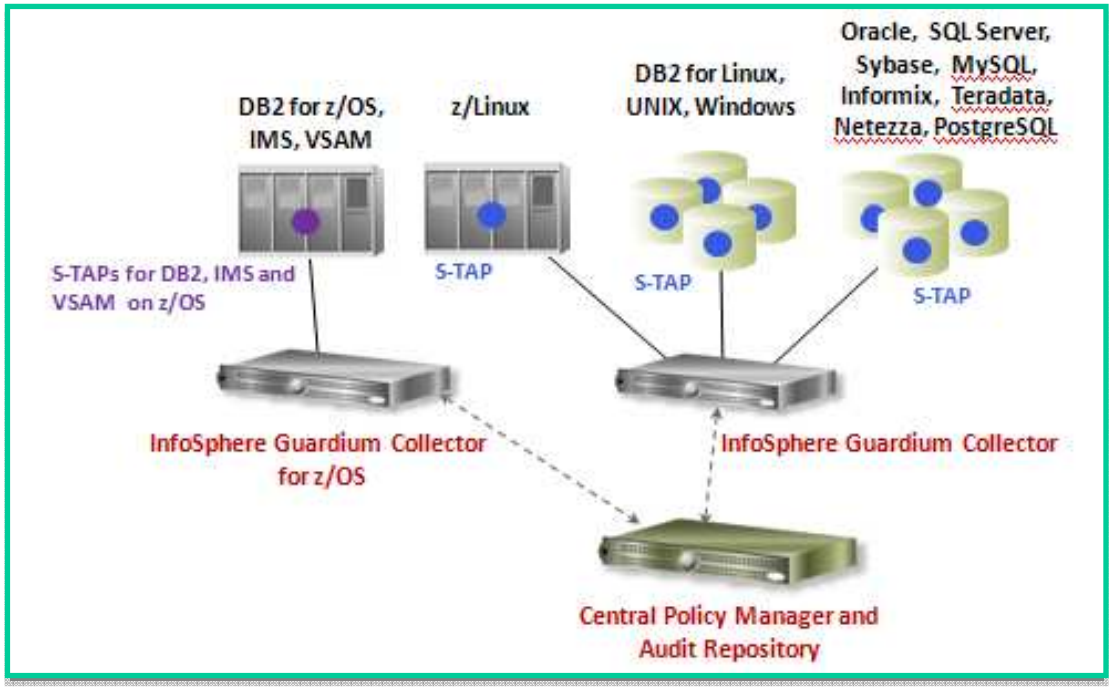
Guardium STAP for IMS on z/OS 8.2

La importancia del soporte a IMS desde el punto de vista de seguridad y compliance



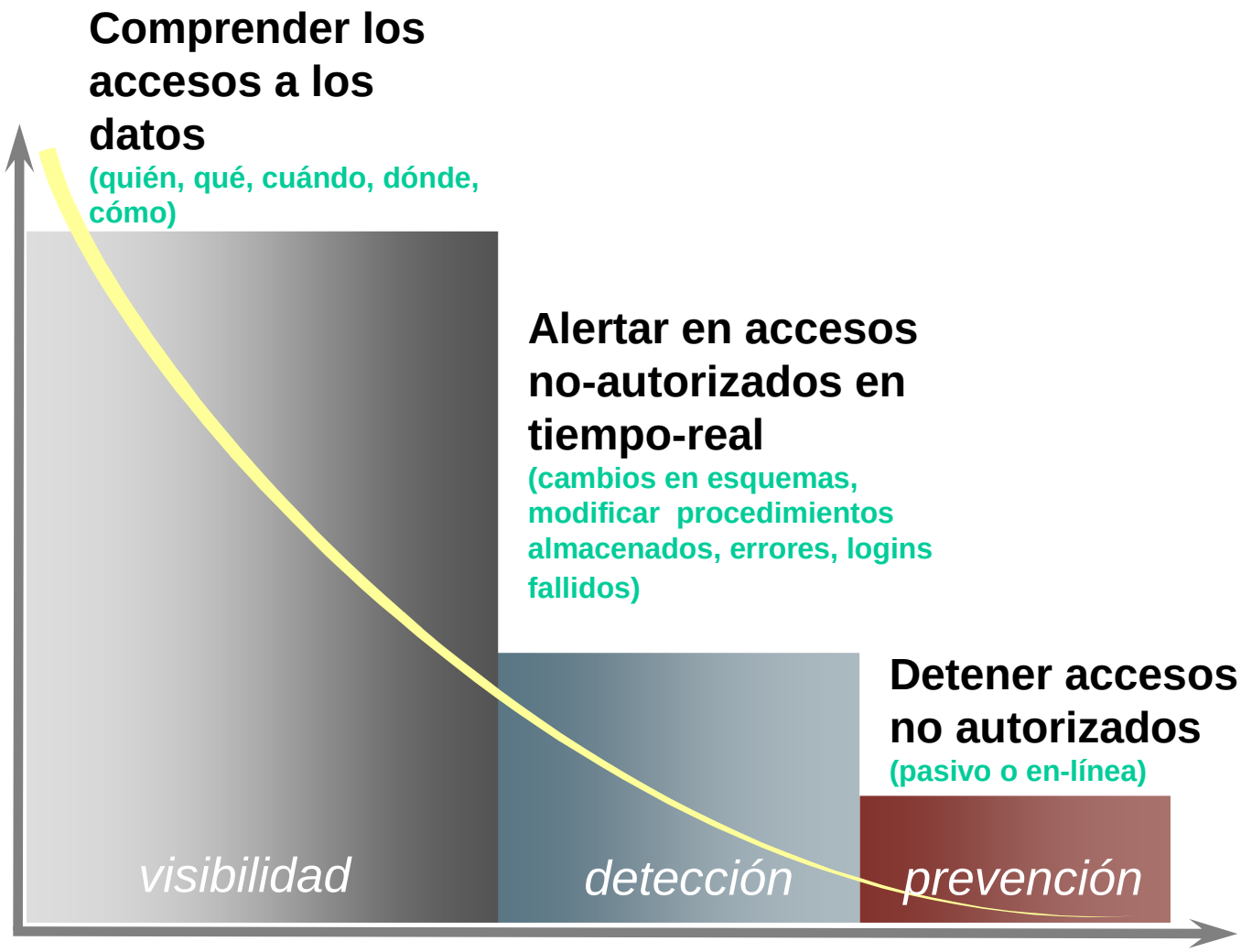
- **IMS es el gestor de bases de datos usado por muchas aplicaciones con acceso a datos sensibles**
  - *La seguridad de los datos es una prioridad*
- **IMS es el gestor que soporta numerosas aplicaciones críticas de la empresa**
  - *Sensible a integridad de datos*
- **Creciente demanda de auditorías que afectan también al IMS**
  - *Necesidad de demostrar controles adecuados*
- **Las empresas tienen preocupaciones similares en sus entornos IMS a los que tienen para otros tipos de gestores**
  - *Monitorizar actividades de usuarios privilegiados*
  - *Automatizar la identificación de violaciones de políticas*
  - *Recoger registro granular de auditoría para análisis forense*
  - *Garantizar la Separación de Funciones*
- **Las empresas están buscando eliminar aproximaciones parciales de seguridad y compliance**

Nuevo S-TAP for IMS on z/OS

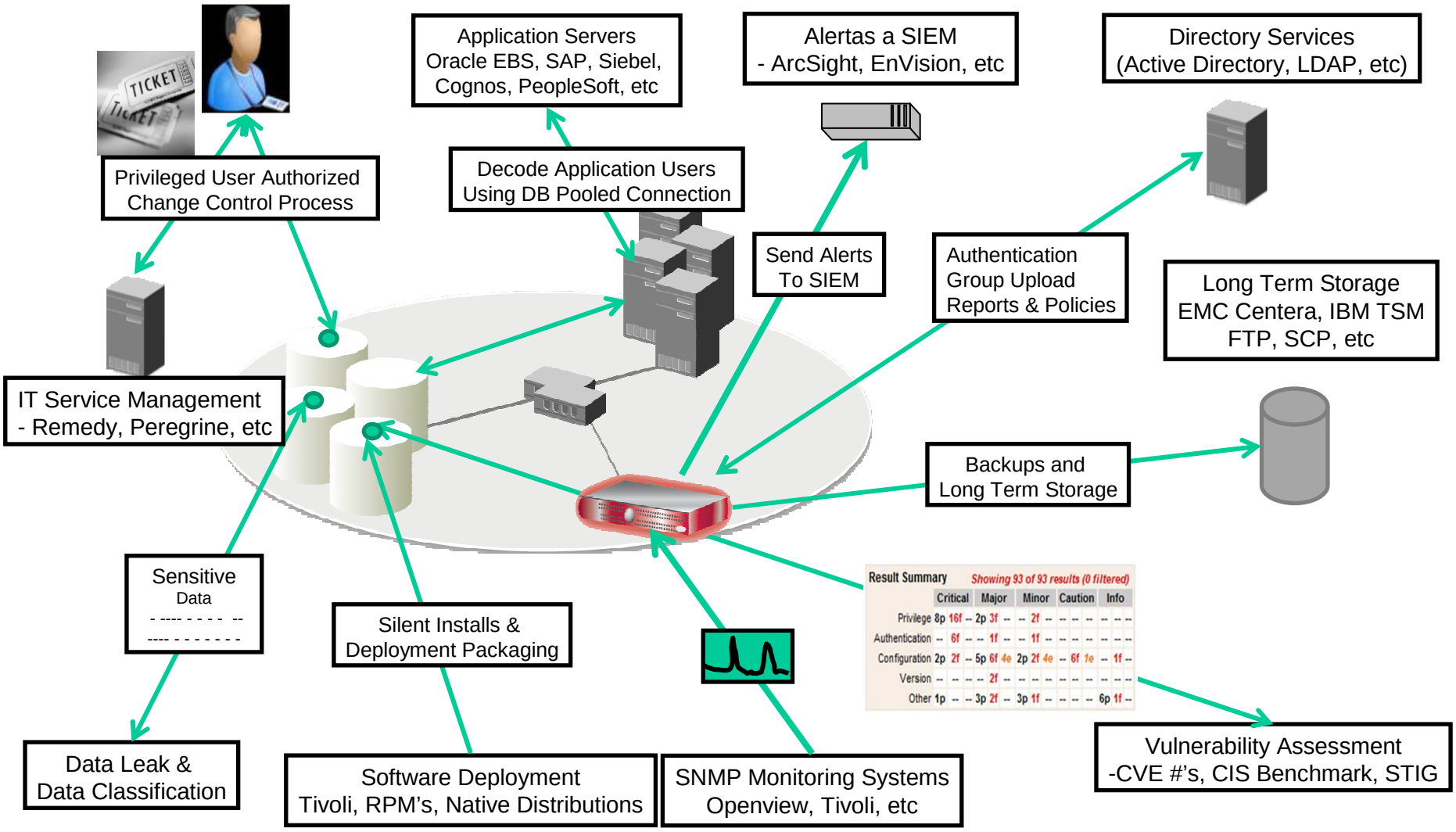


- **Nuevo agente que aprovecha la tecnología de captura de eventos de IBM**
  - *Seguro*
- **Captura de eventos IMS en tiempo real**
  - *DB READs, INSERTs, UPDATEs, DELETEs*
  - *Soporta regiones online y jobs batch*
- **Colector que proporciona funcionalidad consistente con otros agentes**
  - *Registro de auditoría seguro*
  - *Reporting*
  - *Detección de violaciones de políticas*
  - *Workflow de Compliance, etc.*
- **Un agente por instancia**
  - *Servidor de auditoría compartido por varios agentes IMS*

Implantación por fases



Integración con Infraestructura Existente



Guardium for z – Resumen de novedades de la nueva release (V8R2)

- **Nuevo soporte para IMS**
  - Nuevo S-TAP para IMS
  - Captura la actividad de IMS para su envío al Appliance Guardium
  - Monitorización en Tiempo Real de eventos IMS
  - Auditoría extensa de IMS
  - Informes de seguridad y cumplimiento IMS customizables
- **Nuevo soporte para VSAM**
  - Nuevo S-TAP para VSAM
  - Captura la actividad sobre ficheros VSAM para mejorar la monitorización de las bases de datos de la empresa
  - Informes de seguridad y cumplimiento VSAM
- **Soporte mejorado para DB2/z**
  - Mejoras constantes en rendimiento
  - Administración unificada del DB2 S-TAP dentro del appliance Guardium
  - Eliminación del FTP – streaming en tiempo real de todos los eventos
  - Mejoras en capacidades y flexibilidad de filtrado (authorization id's)
- **Soporte mejorado para el Vulnerability Assesment DB2/z**

Resumen de InfoSphere Guardium V8.2

- **InfoSphere Guardium es la única solución de seguridad y compliance que proporciona soporte completo en mainframe – afectando a DB2, IMS y VSAM**
  - Utiliza tecnología madura de mainframe para captura de eventos
- **IBM dispone de una solución líder en el mercado que proporciona capacidades a nivel global de la empresa**
  - Interfaz abierto para plataformas únicas o singulares
  - Completa flexibilidad en opciones de desarrollo
  - Integración con entornos de archivado/TDM
- **Esta release continúa la tendencia de IBM de aumentar la flexibilidad, mejorar el rendimiento y reducir los costes**
- **IBM ha continuado el proceso de integración de InfoSphere Guardium con soluciones importantes de su portfolio, reduciendo los costes y mejorando la seguridad**
  - IMS
  - VSAM
  - Mejoras en soporte a DB2 z/OS
  - InfoSphere Discovery