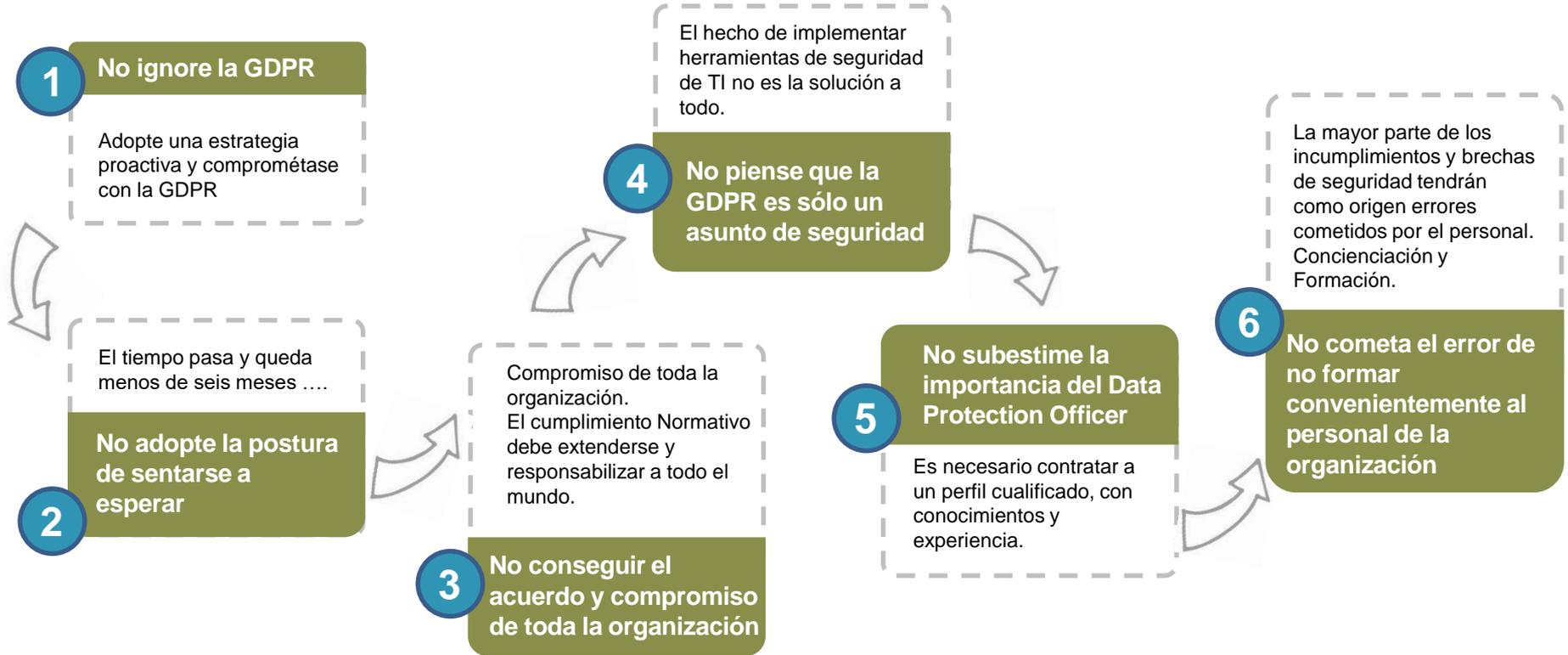


BU Seguridad

Retos GDPR



GDPR: Qué no debemos hacer



Aproximación Logicalis



Servicio de Adecuación a la GDPR

Análisis GAP

- Assessment Tecnológico

Diagnóstico de la situación actual frente a marcos normativos en materia de seguridad



Medidas Tecnológicas

- Plan de Acción Tecnológico
- Análisis y definición de soluciones
- Implantación y adecuación tecnológica



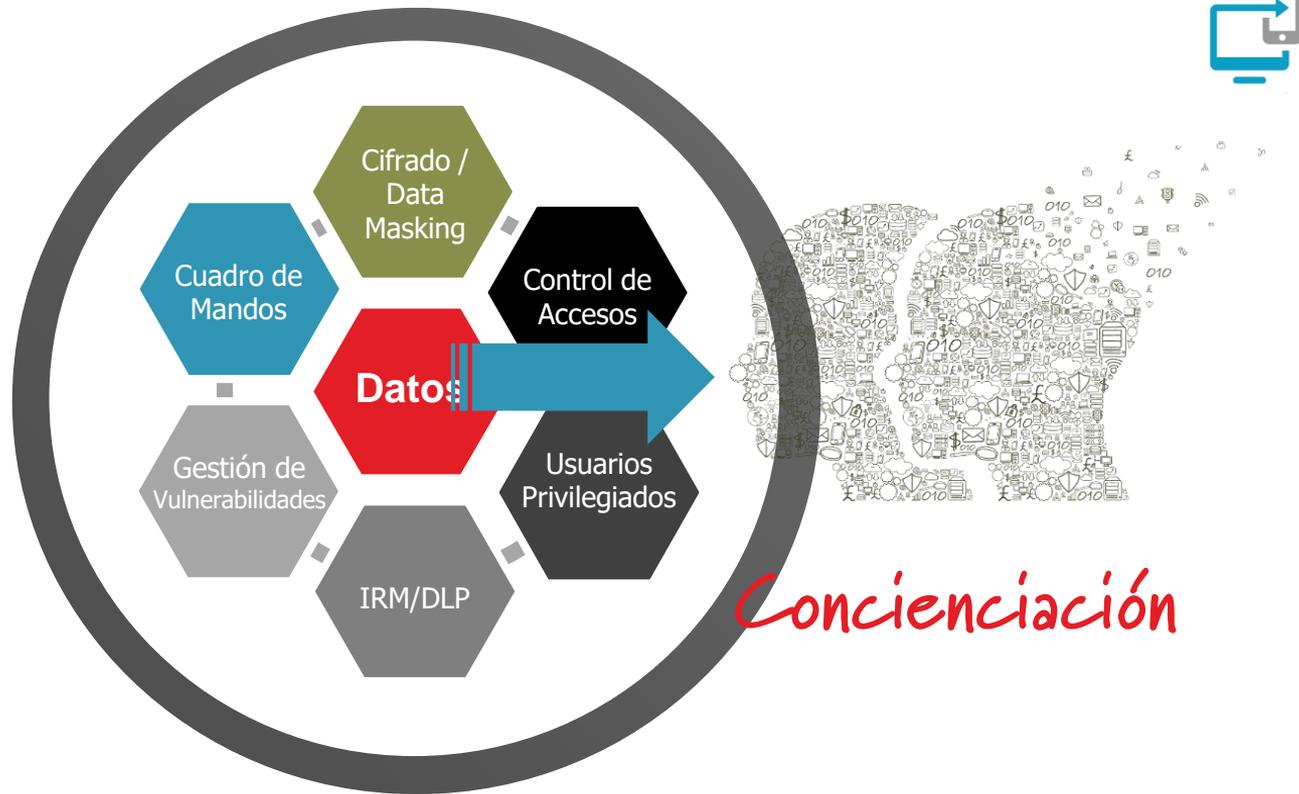
Servicios Gestionados

- Soporte correctivo, preventivo y evolutivo
- Servicios Avanzados de Seguridad
- SOC



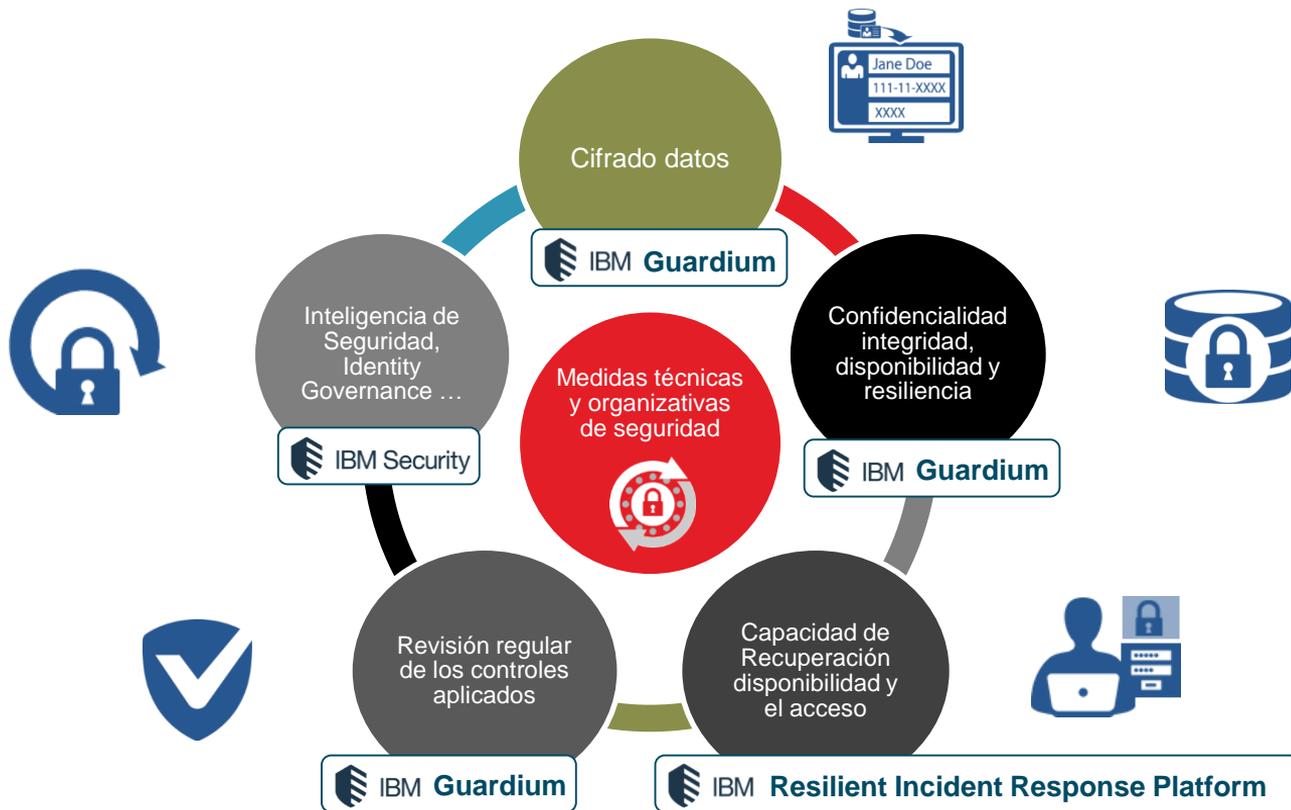
"GDPR: Estrategia y soluciones para encarar el nuevo Reglamento Europeo de Protección de Datos"

Medidas Tecnológicas



"GDPR: Estrategia y soluciones para encarar el nuevo Reglamento Europeo de Protección de Datos"

IBM Security GDPR Privacy



"GDPR: Estrategia y soluciones para encarar el nuevo Reglamento Europeo de Protección de Datos"

Soluciones GDPR

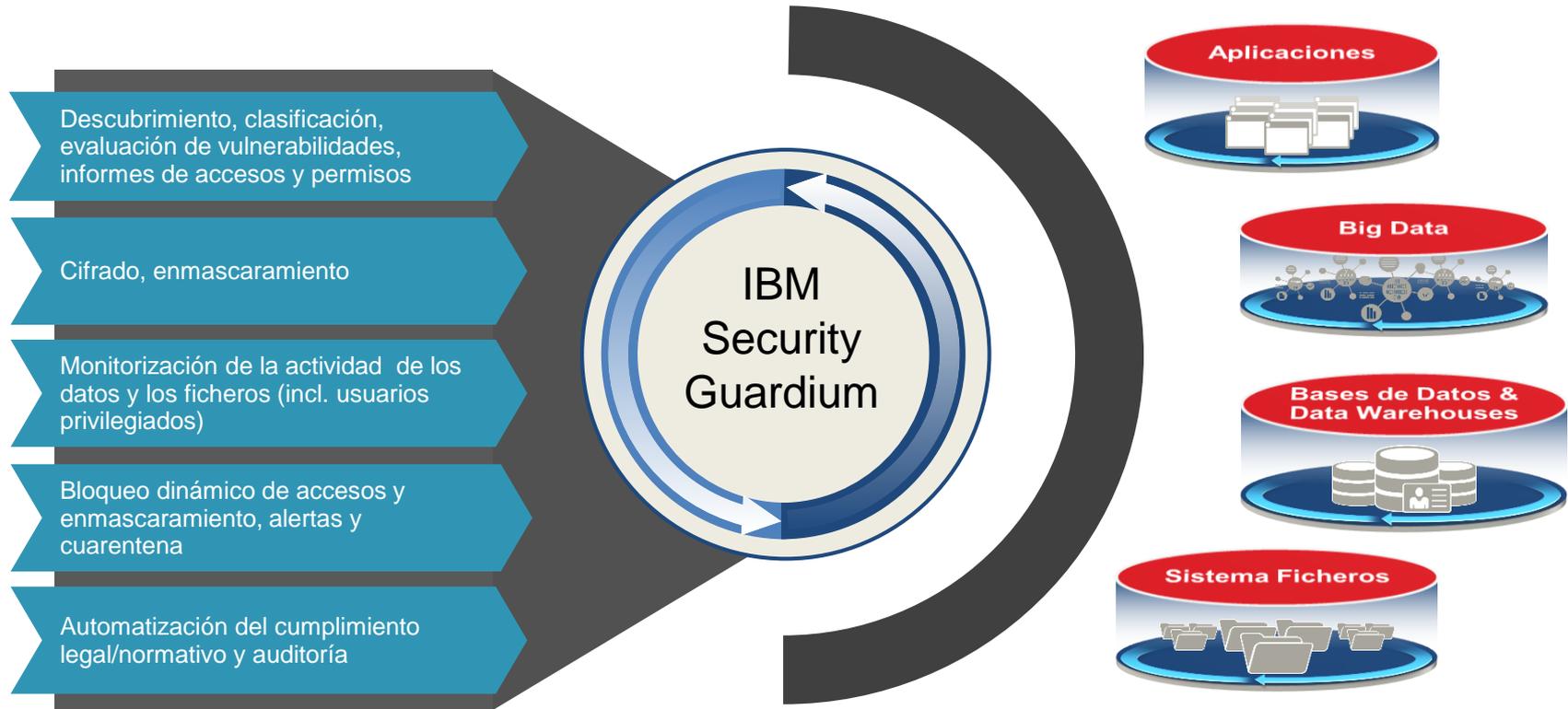
IBM



"GDPR: Estrategia y soluciones para encarar el nuevo Reglamento Europeo de Protección de Datos"

BU Seguridad

Data Protection



"GDPR: Estrategia y soluciones para encarar el nuevo Reglamento Europeo de Protección de Datos"

Data Protection. Ejemplos



**Dónde están
mis datos**



**Escaneo de
vulnerabilidades**

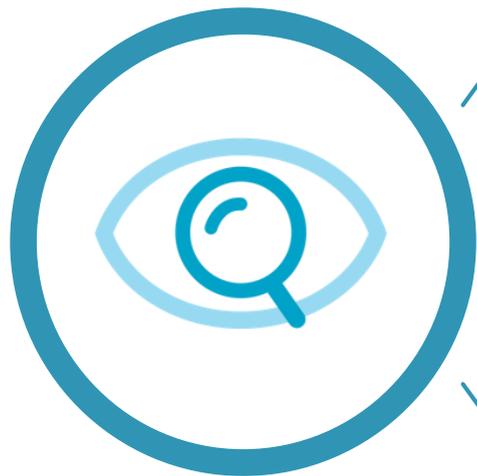


**Monitorización y
Auditoría**

Guardium GDPR Accelerator

Data Protection. Ejemplos (I)

Dónde están mis datos



Soluciones al Desafío de Inventario

Descubrimiento de Activos de Base de Datos

Descubrimiento de Datos Sensibles



Welcome



Setup



Manage



Discover



Harden



Investigate



Protect



Comply



Accelerators



Reports



My Dashboards

Discover Sensitive Data

Discovery Scenarios

- +
-
- GDPR
- GDPR Demo summit
- GDPR Demo summit Oracle
- Quick Start GDPR scenario

Details for: GDPR

Name and description	✔ GDPR	Edit
What to discover	✔ 33 Rules	Edit
Where to search	✔ 1 Datasource	Edit
Run discovery	✔ Last Run: 2017-09-20 05:26:20	Edit
Review report	✔ 22390 matches found	Edit
Audit	Optional: Define auditors for reviewing and signing discovery results	Edit
Schedule	Optional: Define a schedule for the audit process	Edit

Data Protection. Ejemplo (II)

Escaneo de Vulnerabilidades



Plantillas de Escaneo por defecto

Múltiples tecnologías: DB2, AS400, Oracle, SQL, SAP HANA, Cloudera

Reporting y seguimiento para cumplimiento normativo

Data Protection. Ejemplo (II)

IBM Guardium 06:39 User Interface User Interface Search admin, admin-console-only, audit, Baselli, cas, DataPrivacy, fa... Machine Type Standalone

Assessment Test Selections

Tests for Security Assessment GDPR Personal Data Assessment DB2

Select All Unselect All Delete Selected

Type	Test Name	Tuning
<input type="checkbox"/> DB2	Authentication type configuration parameter	CONF Major (n/a) :
<input type="checkbox"/> DB2	Auto-restart after abnormal termination AUTORESTART	CONF Major (n/a) :
<input type="checkbox"/> DB2	CATALOG_NOAUTH parameter is No	CONF Major (n/a) :
<input type="checkbox"/> DB2	CVE-2004-0795	CONF Major (n/a) :
<input type="checkbox"/> DB2	CVE-2004-1372	CONF Major (n/a) :
<input type="checkbox"/> DB2	CVE-2005-0417	CONF Major (n/a) :
<input type="checkbox"/> DB2	CVE-2005-3568	CONF Major (n/a) :

Tests available for addition

Filter By

Test Type Predefined Query based CVE APAR All

Severity Critical Major Minor Caution Info All

Other Include CAS Text

ASTER CLOUDERA MANAGER **DB2** DB2 FOR I DB2 z/OS HIVE INFORMIX MONGODB MS SQL SERVER MYSQL NETEZZA ORACLE POSTGRESQL SAP HANA SYBASE SYBASE IQ TERADATA

"GDPR: Estrategia y soluciones para encarar el nuevo Reglamento Europeo de Protección de Datos"

Data Protection. Ejemplo (II)

IBM Guardium®
Results for Security Assessment: **GDPR Personal Data Assessment DB2**
Assessment executed: 2017-10-25 09:07:41.0

Download PDF Download XML

Tests passing: **43%**
CIS Tests passing: 18/69
STIG Tests passing: 9/17
CVE Tests passing: 19/21

*The above tests passing statistics do not take into account any filtering that may currently be applied, and do not include tests in any status other than passed or failed.

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](#) [B]

Result Summary Showing 271 of 271 results (0 filtered)

	Critical	Major	Minor	Caution	Info
Privilege	3p 39f	2p 8f 2e	-- --	9p 10f	-- --
Authentication	-- --	-- --	-- --	-- --	-- --
Configuration	-- --	1e 31p 7f 153e	-- --	1e 2p 1f 1e	-- --
Version	-- --	1p 1f	-- --	-- --	-- --
Other	-- --	-- --	-- --	-- --	2e

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

Reset Filtering Filter / Sort Controls

Assessment Test Results Compare with other results Showing 271 of 271 results (0 filtered)

Test / Datasource	Result
DB2 Roles granted to PUBLIC Test category: Priv. Severity: Critical Granting to PUBLIC increases the risk of unauthorized entry into the database. Because PUBLIC is accessible by any database user, it is important to understand the exposure it has on all database objects. As any role granted to PUBLIC can potentially allow the compromise of database availability, confidentiality, or integrity, these roles should be restricted according to the needs of the business. Ext. Reference: CIS IBM_DB2 10 v1 1.0 Item #6.4 [VA] DB2INST1	Fail One or more roles are granted to PUBLIC. Recommendation: We recommend you to revoke roles that are granted to PUBLIC. You can use this command to revoke: <u>revoke role <role name> from PUBLIC;</u>

"GDPR: Estrategia y soluciones para encarar el nuevo Reglamento Europeo de Protección de Datos"

Data Protection. Ejemplos (III)

Monitorización y Auditoría



Caso de Uso: Data Breach

Políticas de Auditoría

Análisis de actividad de usuarios en tiempo real

Violación de políticas. Enmascaramiento



Policy Finder ?



- Default Sharepoint Auditing
- GDPR
- Hadoop Demo Security Policy
- Hadoop Policy
- HIPAA
- PCI
- PCI, Oracle EBS
- PCI, SAP
- Privileged Users Monitoring (black list)
- Privileged Users Monitoring (white list)
- QRadarPolicy
- Quick Start GDPR
- SOX
- SOX, Oracle EBS
- Vulnerability & Threats Management
- [DAM] Alert fort data protection dashboard
- [DAM] Query Rewrite Policy
- [DAM] SGATE Terminate and Redact Policy
- [FAM] File Activities Logging - HIPAA
- [FAM] Sensitive Files Deletion - sourcecodes

-- Select an installation action --

[Edit Rules](#)

[Comments](#)

Latest Logs and Violations

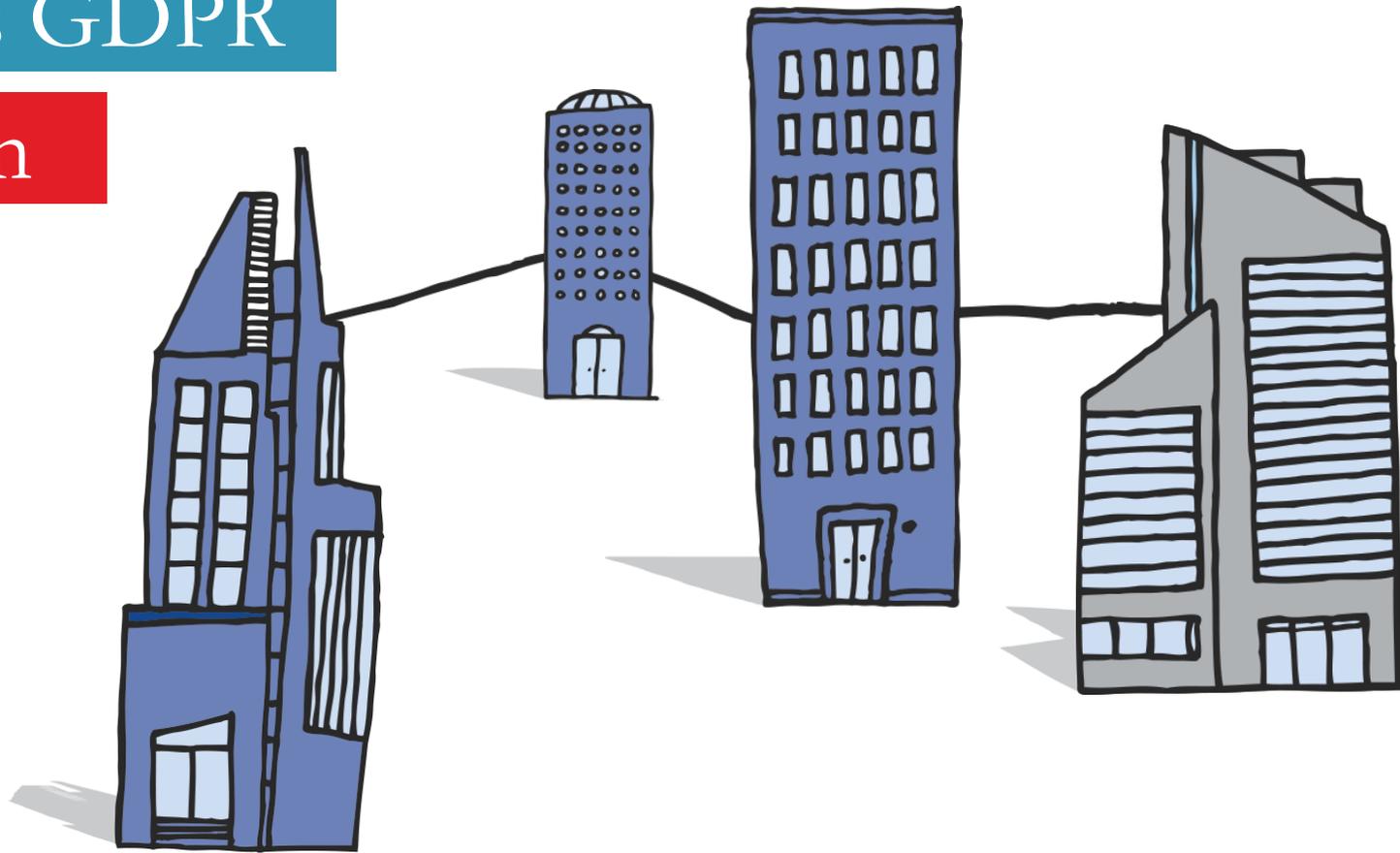
During the last: 5 minutes 1/2 hour 1 hour

Rule	# SQLs	# Viol.	Last Occurrence
Credit Card Numbers, Unauthorized Users - Log Violation	0	0	
DDL Commands, GDPR Personal Data Sensitive Objects - Log Full Details	0	0	

- Setup
- Manage
- Discover
- Harden
- Investigate
- Protect
- Comply
- Accelerators
- Reports
- My Dashboards

Soluciones GDPR

Integración

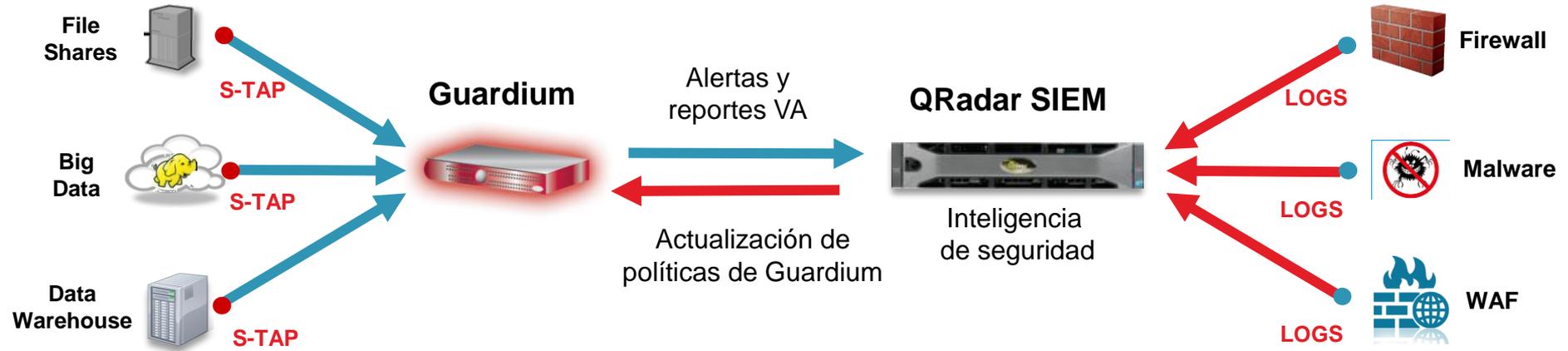


"GDPR: Estrategia y soluciones para encarar el nuevo Reglamento Europeo de Protección de Datos"

BU Seguridad

 **LOGICALIS**
Business and technology working as one

Data Protection & SIEM (I)



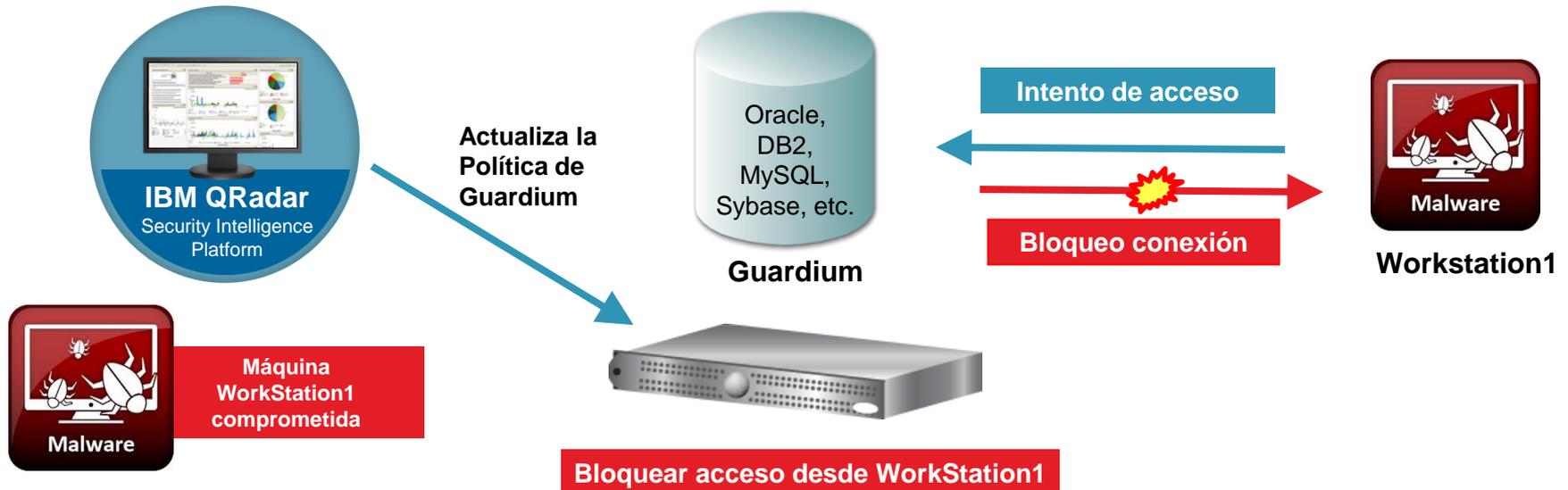
Es posible mantener las políticas de Guardium actualizadas en tiempo real y de forma automática en respuesta a eventos de seguridad de QRadar

Flujo de información bidireccional

Data Protection & SIEM (II)

Caso de Uso

- Detección de una máquina infectada con Malware y bloqueo automático del acceso



Respuesta Incidentes de Seguridad

Los desafíos en la comunicación de brechas de seguridad

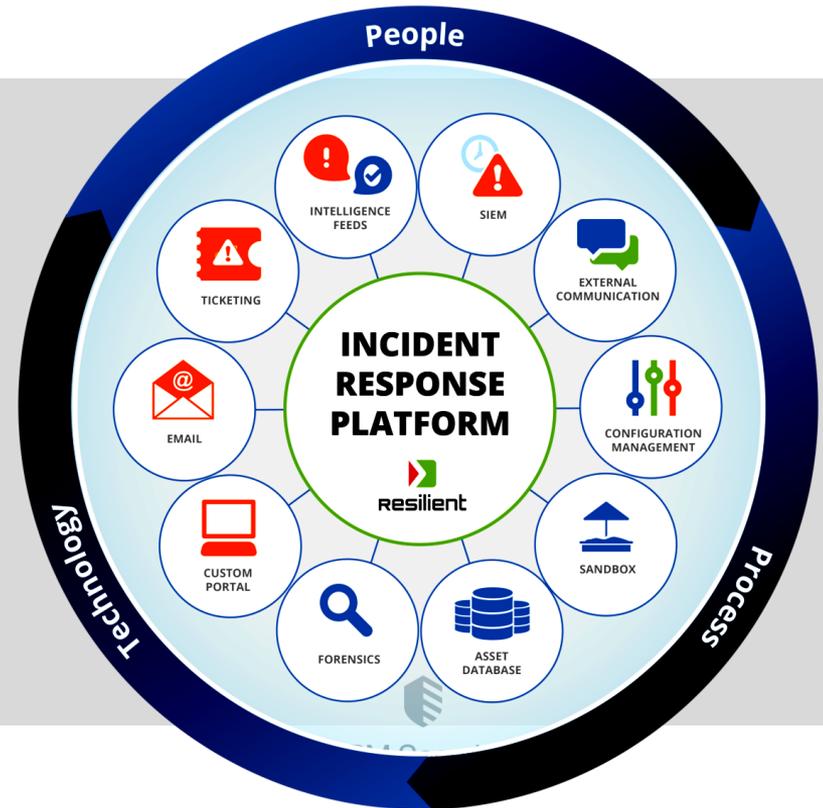
GDPR Obligará a reportar a las autoridades una brecha de seguridad en menos de **72 horas** y a notificar a los clientes afectados por las mismas. Lo que plantea un gran reto en los equipos de seguridad.

Reduce tiempos, mejora la orquestación, facilita la recolección de evidencias

Permitirá a los equipos de seguridad orquestar los procesos de respuesta, y resolver incidentes más rápido y de forma más inteligente. Lo que antes se hacía en días/semanas ahora puede hacerse en horas/días.

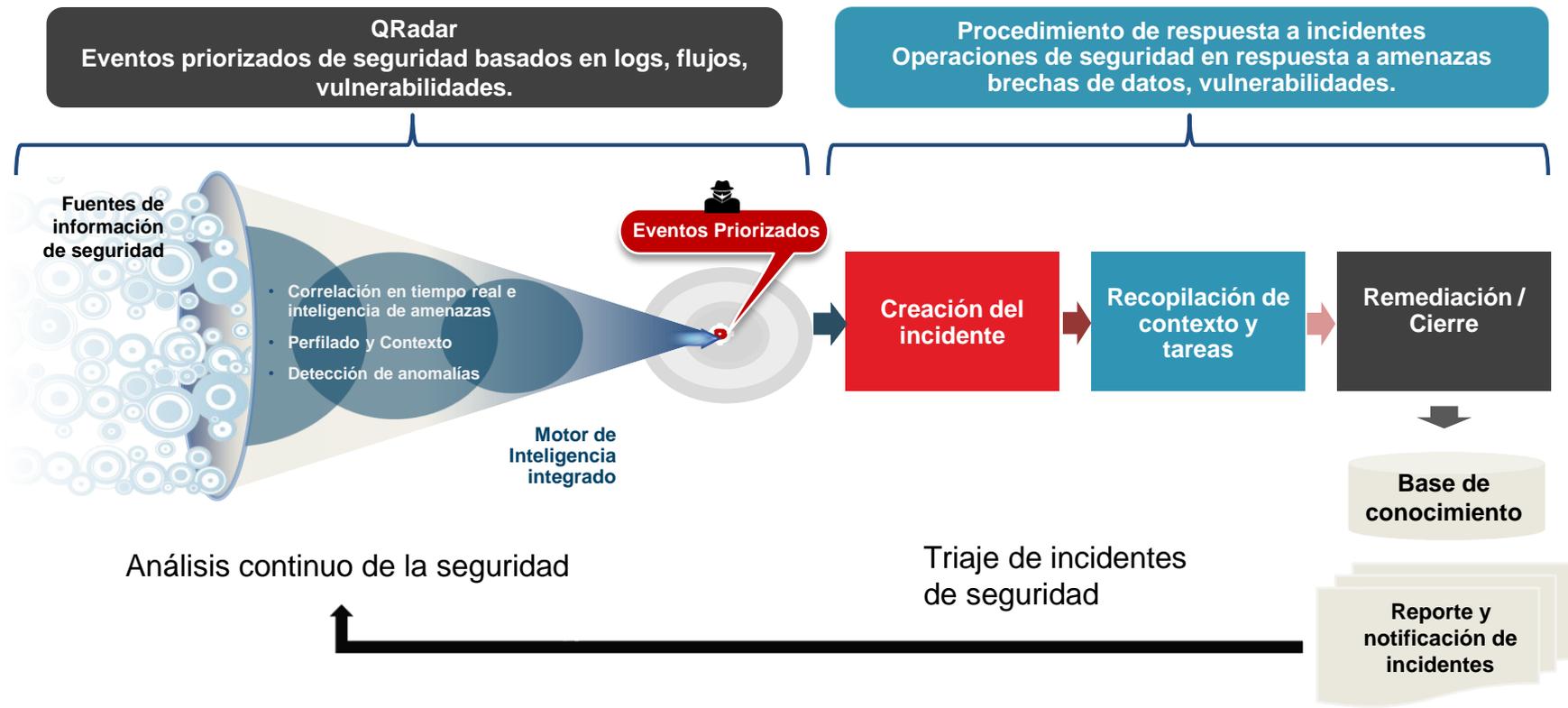
Se integra a la perfección con productos de IBM y de terceros

Además posee funcionalidades específicas para cumplimiento y seguimiento GDPR (GDPR Enhanced Privacy Module).



"GDPR: Estrategia y soluciones para encarar el nuevo Reglamento Europeo de Protección de Datos"

SIEM & Resilient





Business and technology working as one

Próximos pasos ...

Gracias !!!

