

Acelerador PCI

Para el Cumplimiento en Bases de Datos

Soluciones Guardium

Trabajando conjuntamente con otras soluciones de Guardium, el Acelerador PCI acelera el cumplimiento, suministrando:

- **Mapa de Acceso a la Base de Datos del Tarjeta Habiente**

Se provee un mapa grafico entre las estaciones con acceso a las bases de datos de tarjeta habientes y los servidores que la contienen. Este mapa nos permite dar un vistazo las actividades por tipo de acceso, contenido y frecuencia.

- **Tarjeta de Reporte de Cumplimiento PCI**

Una vista detallada de la salud de la seguridad para el acceso a las bases de datos del tarjeta habiente, usado para automatizar el proceso de cumplimiento, mediante una constante fotografía a tiempo real personalizada por el usuario definiendo pruebas, el peso y las evaluaciones.

- **Auditoria completa**

La generación de pistas de auditoría no invasiva y completa, de la utilización de los datos y modificaciones, requeridas para el cumplimiento de la normativa.

- **Planificación Automatizada.**

Programación automatizada del flujo de trabajo de PCI, tareas de auditoria y difusión de informes a los responsables, a través de la empresa, beneficia la rendición de cuentas.

- **Constructor de Referencia de Políticas Dinámicas y el Nivel de Protección de la Base de Datos SQL.**

Desarrollo simplificado y automatizado de las reglas de acceso para la información del tarjeta habiente; seguridad explicita de las políticas con una continua capacidad de refinamiento, además del nivel de control de acceso a la protección de la información SQL.

El Estándar de Seguridad de Datos (DSS por sus siglas en ingles) de la Industria de las Tarjetas de Pago (PCI por sus siglas en ingles) ofrece un acercamiento para salvaguardar la seguridad de la información sensible para todos los tipos de tarjetas de crédito. Este sistema consiste en doce requerimientos. Como resultado de la implementación de este estándar, se obtiene un solo proceso de validación para proteger la información de los tarjeta habientes.

Acelerando el proceso

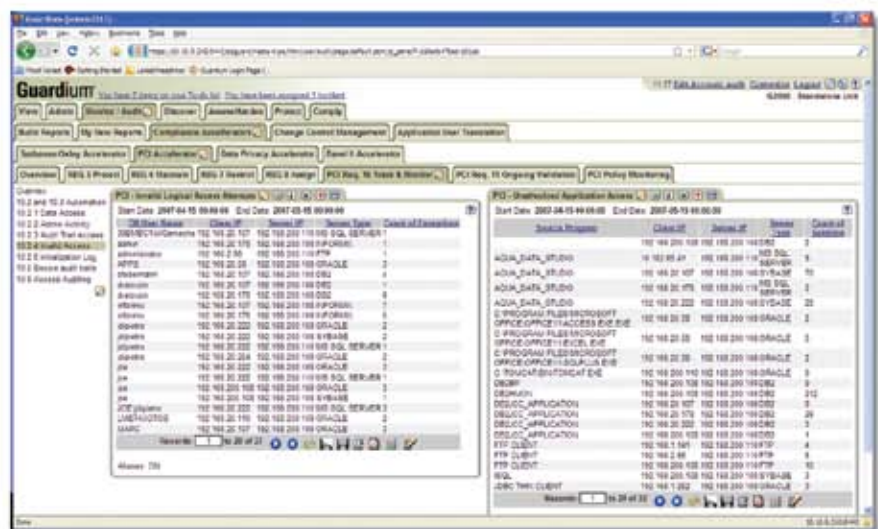
Como parte del crecimiento de Guardium en los aceleradores para el cumplimiento en base de datos, el Acelerador PCI para el Cumplimiento en la Base de Datos simplifica y automatiza los procesos necesarios para apoyar estas directivas y permite la seguridad de la información del tarjeta habiente.

Muchos requerimientos del Estándar en la Protección de Datos de PCI, enfatizan la importancia en el monitoreo a tiempo real y en el rastreo del acceso de la información del dueño de la tarjeta y la continua evaluación de la salud de la seguridad de la base de datos, de la siguiente manera:

- Requerimiento 3: Proteger y almacenar los datos manteniendo solo la mínima información necesaria.
- Requerimiento 6: Asegurar el sistema manteniendo un proceso de control de cambios.
- Requerimiento 7: Acceso limitado a "necesito saber".
- Requerimiento 10: Buscar y monitorear todos los accesos a los recursos de la red y a los datos del tarjeta habiente.
- Requerimiento 11: Probar regularmente las vulnerabilidades de seguridad.
- Requerimiento 12: Mantener y hacer cumplir las políticas de seguridad de la información.

El Acelerador PCI asiste a las organizaciones para establecer controles en el uso y almacenamiento de la información del tarjeta habiente. El sistema puede escanear automáticamente todo el trafico SQL en tiempo real, buscando patrones reconocibles que están contenidos en la banda magnética de la tarjeta. Se pueden establecer reglas de acción para realizar pruebas utilizando patrones definidos por expresiones regulares e.g [0-9]{4}[0-9]{4}[0-9]{4}[0-9]{4}.

Eventos sospechosos reciben una respuesta inmediata y automatizada: bloqueando el almacenamiento o recuperando la pista de datos, enviando notificaciones inmediatas, o guardando la información para una futura investigación y corrección.



Suministrando las herramientas para acelerar el cumplimiento

Adaptadas para abordar el proceso de monitoreo y el control del almacenamiento y acceso de la información del tarjeta habiente, el Acelerador PCI provee una plantilla pre-configurada y otras herramientas, que pueden ser personalizadas para reflejar requerimientos organizacionales específicos.

El reporte predefinido de las plantillas y el flujo de trabajo automatizado, aumenta la visibilidad en las actividades de la base de datos mientras simplifica el descubrimiento de asuntos que puedan requerir una mayor investigación. Las plantillas de reporte pueden ser personalizadas, para reflejar requerimientos específicos de las organizaciones. Esta solución también realiza una auditoría y ayuda a documentar el acceso a la información del tarjeta habiente y establece un ambiente de rendición de cuentas y visibilidad creciente. Las funciones del Acelerador de PCI incluyen:

| TAREA | BENEFICIO |
|---|---|
| Planificar y organizar | Provee reportes que permiten a los usuarios planear el cumplimiento en bases de datos de PCI. El reporte permite a los usuarios observar la información acerca de quien o que toca la información de los tarjeta habientes; fácilmente mapea los servidores de bases de datos de los tarjeta habientes, clientes (pc's), usuarios; verificando que las IDs y cuentas genéricas sean discapacitadas o removidas; asegurando que las IDs compartidos no son usados para actividades de administración del sistema u otras funciones críticas y más |
| Requerimiento PCI 3: Salvaguardar Información Rastreada. | Asiste a las organizaciones a establecer controles acerca del uso y almacenaje de los datos rastreados del tarjeta habiente. El sistema automáticamente puede rastrear todo el tráfico de datos SQL en tiempo real, buscando por patrones reconocibles que están contenidos en las bandas magnéticas. Las reglas de la política pueden ser establecidas para realizar pruebas con patrones. Eventos sospechosos reciben una respuesta automatizada inmediata: bloqueando el almacenamiento de información buscada, mandando notificaciones inmediatas, o guardando la información para futuras investigaciones y correcciones |
| Requerimiento PCI 6: Cambio en la Gestión de Control | Provee una solución poderosa e innovadora para solucionar el problema de la reconciliación en los cambios en el esquema de la base de datos. Guardium permite a los DBAs asociar cambios en los números solicitados con los cambios hechos a la base de datos y después compararlos con las soluciones de control de cambios (Peregrine, Remedy etc) para identificar cambios no autorizados. |
| Requerimiento PCI 10: Búsqueda y Monitoreo | Permite a los usuarios certificar que las actividades de acceso a la base de datos son correctas y que las que están afuera de los parámetros de seguridad del PCI pueden ser, ya sea rectificadas o más investigadas. La funcionalidad provee una variedad de reportes en temas tales como excepciones en el sistema y contraseñas fallidas, auditoría en la actividad de usuarios y acceso a la información del tarjeta habiente por aplicaciones no autorizadas. En adición, esta solución automatiza los flujos de trabajo y difunde el acceso a bases de datos de información en toda la organización. |
| Requerimiento PCI 11: Continúas Evaluaciones de Vulnerabilidad | Incluye una Evaluación a la Salud de la Seguridad que ofrece las herramientas métricas y visuales requeridas para la evaluación continua y el mejoramiento dinámico de los sistemas de seguridad de la base de datos y los procesos. Una vista al tablero de mandos (dashboard) permite a los usuarios en tiempo real e históricamente hacer un mapeo de las medidas de seguridad en contra de métricas preconfiguradas como: Cuentas Compartidas, Inicio de Sesión en Horas no Permitidas, Acceso de Usuario sin Autorización y otras. |