Documento técnico de Oracle
Junio de 2009

Oracle Database 11g: Soluciones rentables para seguridad y cumplimiento normativo

ORACLE

Protección de información delicada

Todo tipo de información, desde secretos comerciales hasta datos financieros e información privada, ha pasado a ser el objetivo de sofisticados ataques provenientes de ambos lados del firewall. Si bien la mayoría de las empresas han implementado tecnologías de firewall, detección de intrusiones y filtro de correo no deseado, para proteger los datos ahora se necesita una estrategia de defensa en profundidad que también incluya el cumplimiento normativo. Con el respaldo de 30 años de experiencia en seguridad, Oracle Database ofrece controles de defensa en profundidad que permiten a las empresas proteger su información de manera transparente. Estos controles otorgan a las empresas la posibilidad de proteger sus datos y asegurarse de lograr el cumplimiento normativo de forma rentable y sostenible.

Impulsores de las medidas de seguridad

El avance de la tecnología dio lugar al surgimiento de Internet y la globalización de la economía, y ha permitido a las empresas reducir los costos y aumentar la productividad considerablemente. Sin embargo, la tecnología también permite enviar amenazas para los datos desde cualquier parte del mundo. Ciertos impulsores del negocio, como la consolidación de la información, la tercerización estratégica y la computación en nube son cada vez más importantes para reducir los costos. Sin embargo, no es posible implementar estos requisitos sin controles de seguridad adecuados y soluciones de seguridad innovadoras. El desafío no es sólo proteger los datos, sino hacerlo de tal manera que permita mantener la escalabilidad, el rendimiento y la elevada disponibilidad de las aplicaciones.

Figura 1. Impulsores de medidas de seguridad en negocios globales

La protección contra la pérdida accidental e intencional de datos por causas internas requiere la implementación de los principios de "necesidad de conocimiento" y de "confiar y verificar". En varios países, como Estados Unidos y Japón, se han aprobado leyes que exigen controles internos de los datos financieros. Asimismo, hay cada vez más normativas sobre privacidad que obligan a cifrar la información personal identificable. Por ejemplo, en los Estados Unidos, más de 40 estados aprobaron algún tipo de ley sobre notificación de violaciones de datos. Al mismo tiempo, algunas iniciativas impulsadas por la industria, como la norma de seguridad de los datos de la industria de tarjetas de pago (PCI), implican la restricción del acceso a información sobre tarjetas de crédito.

Seguridad de defensa en profundidad

La defensa en profundidad conlleva un enfoque holístico de la seguridad de los datos. Por lo tanto, es necesario tener en cuenta todo el ciclo de vida de los datos, dónde se encuentran, qué aplicaciones y qué usuarios tienen acceso a ellos, en qué condiciones ocurre el acceso, y asegurarse de que los sistemas estén configurados adecuadamente y se mantengan así. Los tres elementos clave de este enfoque son el cifrado y enmascaramiento de datos, el control de acceso y el monitoreo:

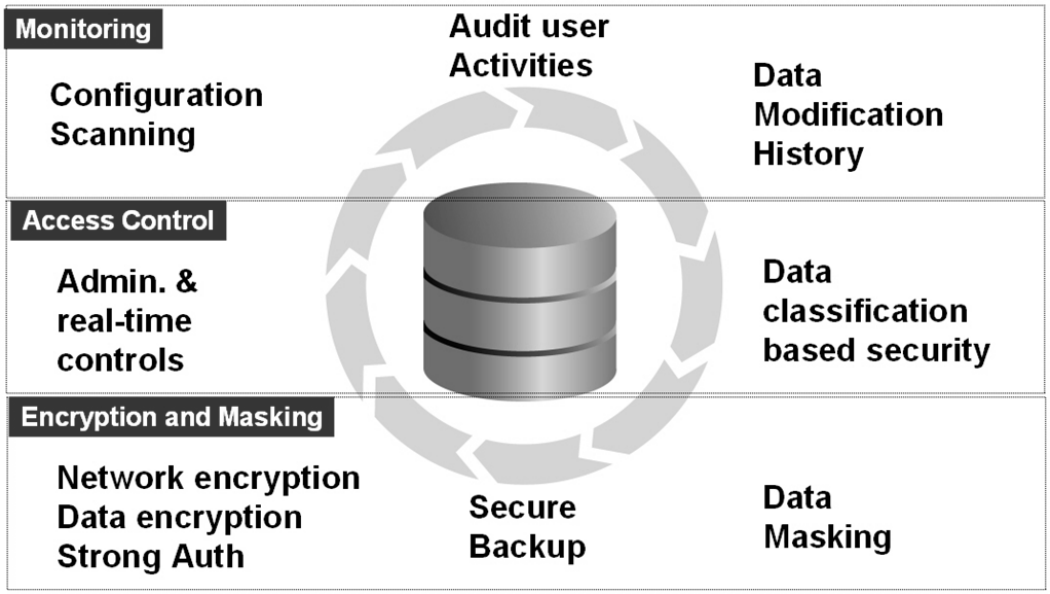

Figura 2. Defensa en profundidad

El cifrado y el enmascaramiento de datos son procesos importantes para proteger los datos fuera del perímetro de control de acceso de la base de datos. Los datos almacenados en discos por debajo de la base de datos y las aplicaciones, los datos utilizados en entornos de prueba y de desarrollo, los datos que se transfieren a través de la red y los datos almacenados en medios de backup requieren una protección que solamente puede obtenerse mediante el cifrado y el enmascaramiento. El descarte de unidades de disco y la presencia de superusuarios en el sistema operativo abren la puerta al acceso sin impedimentos a ciertos datos delicados sin que se realice una autenticación y ni se apliquen controles de acceso de la base de datos. El envío de datos de producción a otros departamentos para pruebas y desarrollo implica una exposición innecesaria de los datos delicados a personas que no tienen una verdadera necesidad de conocimiento. Sin duda, los datos que se transmiten por una red están expuestos a un elevado riesgo de acceso no autorizado.

En la actualidad, los controles de acceso más allá de las aplicaciones son imprescindibles para que la empresa pueda obtener los beneficios de la consolidación de la información, la tercerización internacional y la computación en la nube. Hasta el momento, el diseño de las aplicaciones apuntaba a escalar a los requisitos de Internet y ofrecer acceso funcional según el rol del usuario. Hoy en día, sin embargo, las reglamentaciones y las leyes sobre privacidad exigen que se limite el acceso a los datos de las aplicaciones, incluso para el administrador de la base de datos y, especialmente, para las herramientas ad hoc que permiten burlar las aplicaciones.

Si bien el cifrado y el control de acceso son componentes clave de la protección de datos, incluso los mejores sistemas de seguridad necesitan la ayuda de un sistema de monitoreo. Así como las cámaras de video sirven como complemento para las alarmas sonoras en los hogares y las empresas, el monitoreo ofrece información complementaria sobre quién, qué y cuándo se accedió a los datos para los sistemas de cifrado, enmascaramiento y control de acceso.

Solución de seguridad de defensa en profundidad de Oracle

Oracle ofrece una solución de defensa en profundidad integral y transparente que satisface los desafíos asociados a las iniciativas comerciales y el complejo entorno normativo que rige la economía mundial de hoy en día.

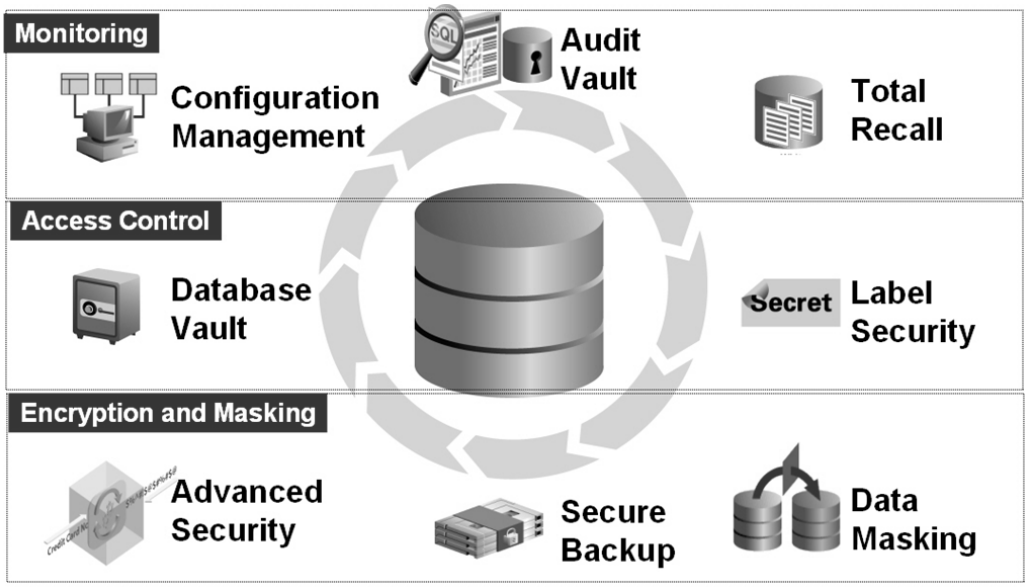

Figura 3. Solución de defensa en profundidad de Oracle

Cifrado y enmascaramiento

- Oracle Advanced Security ofrece un cifrado transparente de los datos almacenados y de los datos en tránsito.

- Oracle Secure Backup es una solución de backup en cinta que cifra las bases de datos y los datos del sistema de archivos.

- Oracle Data Masking des-identifica los datos de producción antes de transferirlos a entornos de prueba o a socios.

Control de acceso

- Oracle Database Vault ofrece control de acceso para los usuarios administrativos y con privilegios, y controles en tiempo real de la actividad de la base de datos.

- Oracle Label Security ofrece control de acceso según la clasificación de los datos.

Monitoreo

- Configuration Management de Oracle Enterprise Manager analiza la base de datos y el sistema de archivos en busca de parámetros de configuración relacionados con la seguridad.

- Oracle Audit Vault consolida los datos de auditoría de varios servidores a fin de llevar un registro de la actividad de los usuarios, y crea informes y alertas sobre actividades sospechosas.

- Oracle Total Recall ofrece un historial de los cambios realizados sobre los datos delicados.

Cifrado y enmascaramiento

Cifrado de datos transparente

Oracle ofrece sólidas soluciones de cifrado que permiten proteger los datos delicados contra el acceso no autorizado en el ámbito del sistema operativo y contra el robo de hardware o medios de backup. Oracle Transparent Data Encryption (TDE) permite satisfacer requisitos de privacidad y de la industria de tarjetas de pago mediante el cifrado de la información personal identificable, como números de seguridad social y de tarjetas de crédito.

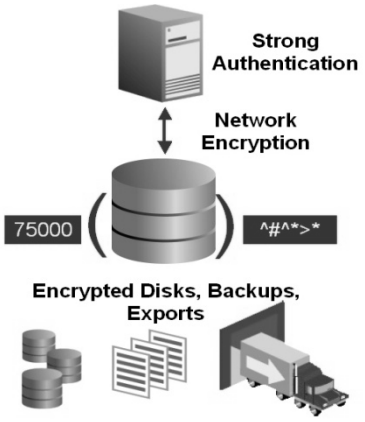

Figura 4. Cifrado y autenticación firme de Oracle

Oracle permite cifrar de forma transparente columnas específicas de datos delicados mediante el cifrado de columnas TDE, o cifrar aplicaciones completas mediante el cifrado de espacios de tablas TDE. Con Oracle Enterprise Manager, es posible cifrar fácil y rápidamente una columna o crear un espacio de tablas completamente cifrado para almacenar todas las tablas de aplicaciones. El cifrado TDE es totalmente transparente para las aplicaciones existentes y no requiere activadores, visualizaciones ni otros cambios de aplicaciones. Se cifran los datos de forma transparente cuando se escriben en el disco y se descifran de forma transparente una vez que se autenticó correctamente al usuario de la aplicación y se aprobaron todos los controles de autorización. Las rutinas de backup de la base de datos ya implementadas siguen en funcionamiento, mientras que los datos se conservan cifrados en el backup. Para cifrar backups de bases de datos completas, se puede usar TDE en combinación con Oracle RMAN a fin de cifrar los backups en el disco. El cifrado de columnas TDE y el cifrado de espacios de tabla TDE cuentan con la certificación para aplicaciones Siebel, PeopleSoft y Oracle E-Business Suite.

Oracle Database 11g también permite almacenar la clave maestra de cifrado de TDE externamente en un módulo de seguridad de hardware (HSM) mediante la interfaz

estándar PKCS#11. Esta forma de almacenamiento ofrece un mayor nivel de seguridad para proteger la clave maestra de TDE.

Cifrado de datos en tránsito

Oracle Advanced Security ofrece una solución fácil de implementar que protege todas las comunicaciones con Oracle Database a través del cifrado SSL/TLS y del cifrado de red nativo para las empresas que no cuentan con una infraestructura de PKI. Es posible configurar Oracle Database para que rechace las conexiones de los clientes que no cifren los datos, o que permita ciertas conexiones sin cifrado a fin de otorgar flexibilidad a la implementación. Para simplificar la configuración de seguridad de la red, es posible usar la herramienta de administración Oracle Network Configuration, que permite a las empresas implementar con facilidad el cifrado de red sin necesidad de hacer cambios en la aplicación.

Protección de cintas de backup

Con frecuencia, el robo o la pérdida de cintas ocasiona la pérdida de datos delicados. Oracle Secure Backup cifra las cintas y permite centralizar la administración de los backups en cinta para todo el entorno de Oracle, además de proteger la base de datos de Oracle y los datos del sistema de archivos UNIX, Linux, Windows y Network Attached Storage (NAS) asociados. Oracle Secure Backup se integra con Oracle Database mediante Recovery Manager (RMAN), que admite de la versión Oracle9*i* a la versión Oracle Database 11*g*. Gracias a esta integración optimizada, es posible realizar backups más rápidos que los servicios de administración de medios similares, con un menor uso del CPU.

Oracle Data Masking

Oracle Data Masking ayuda a las empresas a cumplir con las reglamentaciones sobre privacidad y protección de los datos. Con Oracle Data Masking, la información delicada, como números de tarjeta de crédito o de seguridad social, se reemplaza por valores realistas pero no reales. De esta forma, es posible usar sin riesgos los datos de producción para desarrollo, pruebas o uso compartido con socios de tercerización o socios internacionales para otras tareas que no son de producción. Oracle Data Masking usa una biblioteca de plantillas y reglas de formato, y realiza una transformación homogénea de los datos a fin de mantener la integridad referencial para las aplicaciones.

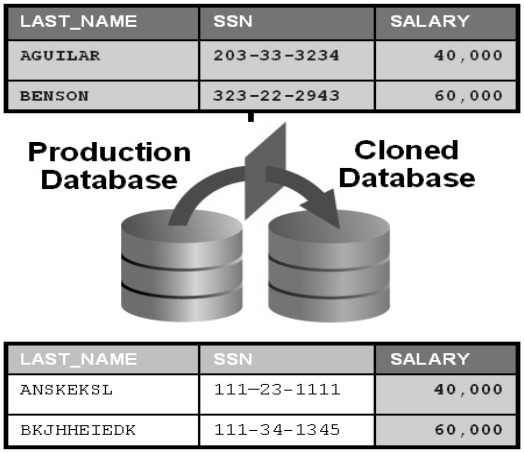

Figura 5. Oracle Data Masking

Control de acceso

Oracle Database ofrece potentes funciones para otorgar y revocar permisos respecto de los objetos de base de datos para los distintos usuarios y roles. Sin embargo, debido a las nuevas amenazas y desafíos, los clientes ahora buscan la separación de tareas, incluso para los administradores, el control de acceso en tiempo real sobre los usuarios y lo que pueden hacer en las bases de datos, y la posibilidad de implementar estas soluciones en las aplicaciones existentes.

Control de usuarios con privilegios

Los administradores de TI, de bases de datos y de aplicaciones ocupan puestos dentro de la empresa que requieren un gran nivel de confianza. Sin embargo, el cumplimiento normativo, la tercerización, la consolidación de aplicaciones y la creciente preocupación por las amenazas internas han llevado a aplicar exigentes requisitos para controlar el acceso a los datos de aplicaciones delicados. Con Oracle Database Vault, las empresas pueden colocar las tablas o los datos de aplicaciones delicados en un dominio a fin de impedir que los usuarios con privilegios tengan acceso a ellos. Los administradores pueden seguir realizando el ajuste del rendimiento y otras tareas de administración de la base de datos, pero no pueden ver ni modificar los datos delicados.

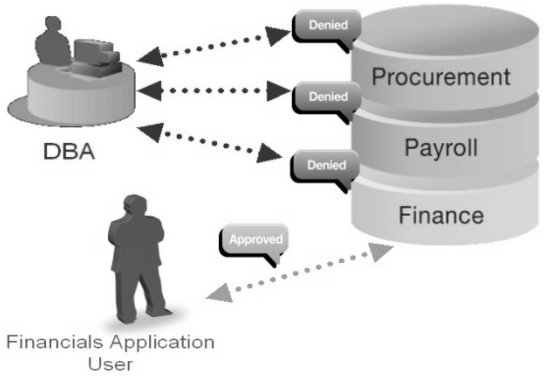

Figura 6. Controles de usuarios con privilegios

Controles de acceso en tiempo real

Oracle Database Vault aumenta notablemente la seguridad al limitar quién, cuándo, dónde y cómo se accede a los datos, las aplicaciones y las bases de datos. Varios factores, como la dirección IP, el horario y el método de autenticación, pueden utilizarse de forma flexible y adaptable para aplicar un control de acceso sin realizar cambios en las aplicaciones. Por ejemplo, se puede restringir el acceso a una capa media específica creando una “ruta de confianza” hasta los datos de aplicaciones e impidiendo el uso de herramientas ad hoc. Es posible usar Oracle Database Vault para habilitar políticas de seguridad adicionales para la mayoría de los comandos SQL.

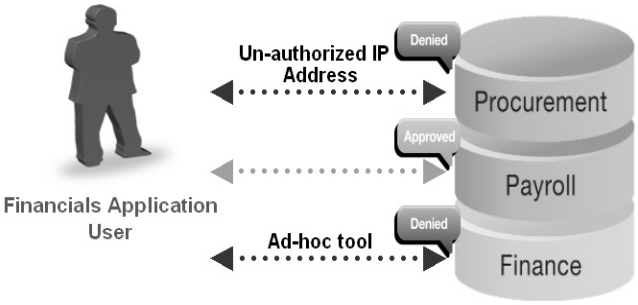

Figura 7. Controles de acceso en tiempo real

Separación de tareas

Oracle Database Vault incluye tres responsabilidades diferentes listas para usar para actividades de seguridad, administración, gestión de cuentas y administración diaria de la base de datos. Por ejemplo, Oracle Database Vault puede bloquear a un DBA e impedir que cree un nuevo usuario si no tiene la responsabilidad adecuada. Las empresas con recursos limitados pueden configurar varias cuentas y seguir aprovechando la separación de tareas implementada con Database Vault. Oracle Database Vault está disponible para Oracle 9i versión 2, Oracle Database 10g versión 2 y Oracle Database 11g. Las políticas listas para usar son compatibles con diversas aplicaciones, incluidas E-Business Suite, PeopleSoft y Siebel.

Seguridad según la clasificación de los datos

Los privilegios tradicionales respecto de las bases de datos, como *seleccionar, insertar, actualizar* y *eliminar* se detienen en el nivel del objeto. Por ejemplo, se puede otorgar un permiso a un usuario para seleccionar en la tabla de clientes, pero no en un subconjunto de filas dentro de la tabla de clientes, de forma tal que el vendedor solamente tenga acceso a los registros de los clientes de su territorio.

Oracle Label Security protege los datos mediante la asignación de una etiqueta de datos a cada fila. Para tener acceso a una fila protegida por una etiqueta de datos, el usuario debe contar con la etiqueta de usuario correspondiente. De acuerdo con la política de la empresa, es posible usar Oracle Label Security para crear políticas que controlen el acceso según la jerarquía, los grupos y los compartimentos.

Las empresas que requieren un elevado nivel de seguridad usan Label Security para organizar en compartimentos el acceso a los datos delicados y confidenciales

almacenados en la misma tabla de aplicaciones. Esta compartimentación se suele denominar seguridad de diversos niveles (MLS). Las organizaciones comerciales pueden usar las etiquetas de datos para compartimentar los datos que se usan en aplicaciones multiempresa, hosting, software como servicio y otras medidas de seguridad.

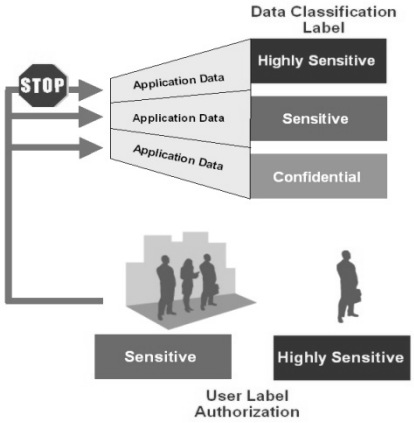

Figura 8. Controles de acceso en tiempo real

Las políticas funcionan como contenedores lógicos de las etiquetas de datos, las etiquetas de usuarios, los parámetros de implementación y los objetos protegidos. En las implementaciones empresariales, es posible administrar centralmente las etiquetas de usuario desde Oracle Identity Management. Asimismo, pueden adjuntarse etiquetas de datos como columnas *ocultas* para las tablas de aplicaciones y permitir que las sentencias de *actualización* e *inserción* sigan funcionando sin modificaciones. Label Security ofrece varias opciones de implementación, como exigir el control de acceso para las operaciones de *selección* y *actualización*, y es compatible con los modelos de usuarios de las aplicaciones comunes.

Las etiquetas de usuario pueden emplearse como factores dentro de las reglas de comando de Oracle Database Vault. Esta excelente función expande los conceptos de Label Security más allá del control de acceso a filas tradicional e incluye los niveles de base de datos y aplicaciones. Por ejemplo, es posible personalizar la separación de tareas a partir de la etiqueta de usuario de un administrador dentro de una regla de Database Vault. Oracle Label Security puede usarse con las aplicaciones ya implementadas, incluso con Oracle E-Business Suite.

Monitoreo

Configuration Management Pack para cumplimiento normativo

La administración de configuración es un componente fundamental de las operaciones diarias de IT de cualquier empresa. Oracle Configuration Management Pack es el eje de la capacidad de Oracle Enterprise Manager para administrar configuraciones y automatizar los procesos de IT. Un componente clave de esta solución es la consola de cambios de configuración, que permite reducir los costos y mitigar los riesgos gracias a la automatización de la detección, la validación y la creación de informes de cambios de configuración autorizados y no autorizados.

Evaluaciones del cumplimiento normativo

La evaluación proactiva de las principales áreas de cumplimiento normativo, como seguridad, configuración y almacenamiento, ayuda a identificar las posibles vulnerabilidades y los sectores donde no se están implementando las mejores prácticas. Oracle Configuration Management Pack cuenta con más de 200 controles de políticas incorporados y ofrece al administrador la posibilidad de definir sus propias políticas personalizadas.

Oracle Enterprise Manager efectúa un seguimiento de las infracciones de estas políticas de forma similar a las métricas de rendimiento. Es posible aplicar reglas de notificación y asignar medidas correctivas a las infracciones. Por ejemplo, si una base de datos incluye un nombre de usuario o una contraseña conocidos, o si se detecta un puerto abierto en el servidor de aplicaciones, se puede definir una medida correctiva que desactive automáticamente la cuenta y cierre el puerto.

Esta aplicación proactiva se complementa con informes de cumplimiento normativo. Estos informes indican el índice de cumplimiento de los objetivos. Es posible ver el índice de cumplimiento a lo largo de un período y obtener detalles sobre las infracciones y el impacto para cada objetivo. La integración con soluciones de resolución de problemas permite enviar automáticamente la información sobre las infracciones de políticas al sistema de soporte y crear tickets para los incidentes sin necesidad de intervención manual. El cuadro de mando de cumplimiento normativo ofrece a los administradores una visualización rápida de cómo los sistemas cumplen las mejores prácticas de seguridad y les permite ver detalles sobre tal cumplimiento. También

pueden ver las tendencias históricas y, así, efectuar un seguimiento del progreso del cumplimiento a lo largo del tiempo.

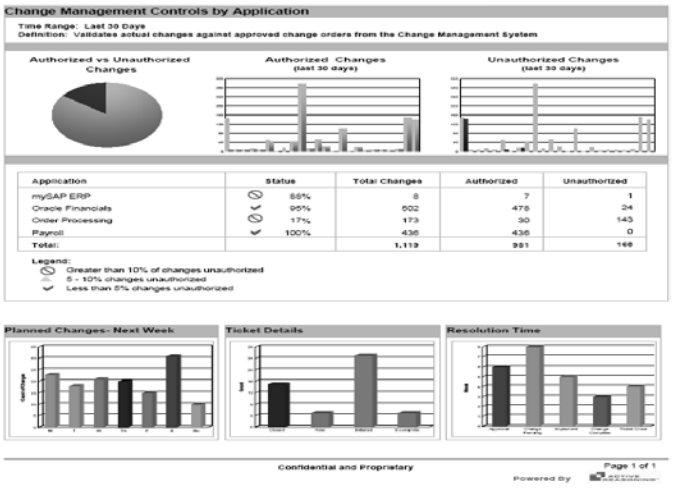

Figura 9. Supervisión de configuración

Monitoreo de las actividades de los usuarios

Para cumplir con las directivas de Sarbanes-Oxley (SOX), de la industria de las tarjetas de pago (PCI) y otras directivas de privacidad regionales, las empresas no sólo deben proteger la información delicada, sino que también deben supervisar el acceso a tal información para garantizar el cumplimiento y detectar amenazas potenciales. El análisis de numerosas infracciones de datos ha demostrado que las auditorías ayudan a detectar problemas tempranamente y, por lo tanto, reducir el impacto financiero.

Realizar auditorías de los usuarios administrativos y con privilegios es una parte esencial de la estrategia de defensa en profundidad. Sin embargo, en la actualidad, el uso de los datos de auditoría como recurso de seguridad sigue siendo un proceso prácticamente manual, en el cual el personal de seguridad de IT y de auditoría debe indagar en grandes cantidades de datos de auditoría dispersos. Oracle Audit Vault reduce el costo y la complejidad del cumplimiento normativo y ayuda a detectar actividades sospechosas gracias a la recopilación y la consolidación transparente de los datos de auditoría, lo cual ofrece valiosa información sobre *quién* hizo *qué* sobre *cuáles* datos y *en qué momento*, incluso sobre los usuarios con privilegios que tienen acceso directo a la base de datos.

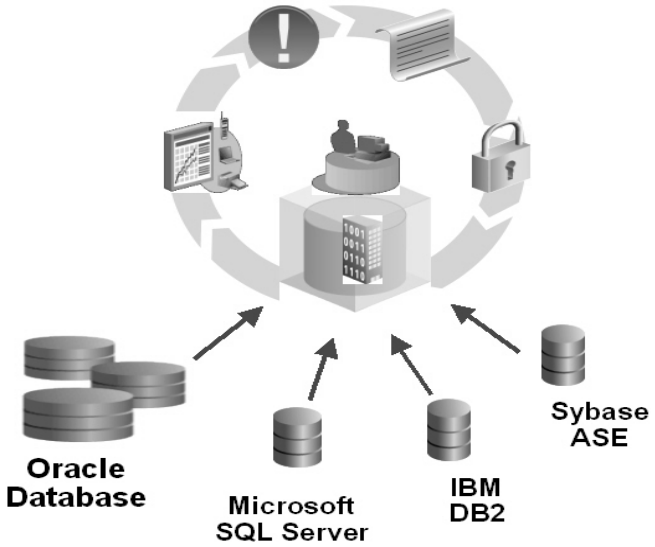

Figura 10. Oracle Audit Vault

Los informes, las notificaciones de alerta y la administración centralizada de políticas de auditoría de Oracle Audit Vault permiten reducir significativamente los riesgos de amenazas internas y el costo del cumplimiento normativo. Oracle Audit Vault aprovecha las tecnologías de seguridad de base de datos y de almacenamiento de datos líderes del sector creadas por Oracle para administrar, analizar, almacenar y archivar grandes cantidades de datos de auditoría.

Oracle Audit Vault ofrece informes de evaluación de auditoría estándar que abarcan a los usuarios con privilegios, la administración de cuentas, los roles y los privilegios, la administración de objetos y la administración del sistema en toda la empresa. Es posible definir informes basados en parámetros, por ejemplo, para mostrar la actividad de inicio de sesión de los usuarios en varios sistemas y dentro de períodos específicos, como los fines de semana. Oracle Audit Vault ofrece un esquema abierto de almacenes de auditoría al que es posible acceder desde Oracle BI Publisher o desde herramientas de creación de informes de otros proveedores.

Las alertas de eventos de Oracle Audit Vault ayudan a mitigar los riesgos y proteger contra amenazas internas mediante la notificación proactiva de actividades sospechosas en toda la empresa. Oracle Audit Vault monitorea continuamente los datos de auditoría entrantes y los evalúa según las condiciones de alerta establecidas. Es posible asociar

alertas a cualquier evento de base de datos que se audite, incluidos los eventos del sistema como cambios en las tablas de aplicaciones, otorgamiento de roles y creación de usuarios con privilegios en sistemas delicados.

Figura 11. Informes de Oracle Audit Vault

Oracle Audit Vault recopila datos de auditoría de la base de datos a partir de las bases de datos Oracle9*i* y superiores, así como de SQL Server 2000 y 2005, Sybase ASE 12.5 - 15.0 e IBM DB2 8.2 y 9.5.

Historial de datos y retención

Las reglamentaciones y normativas como SOX, HIPAA y BASEL–II exigen la retención de datos históricos. Además, las empresas son cada vez más conscientes del gran valor de los datos históricos como ayuda para comprender las tendencias de mercado y el comportamiento de los clientes.

Las empresas necesitan un mecanismo eficaz para retener los datos por más tiempo sin necesidad de reescribir aplicaciones, incluir soluciones de software personalizadas o de otros proveedores o realizar gastos administrativos adicionales. Total Recall de Oracle Database 11g satisface estos desafíos mediante la retención y la administración integral y segura de todos los datos históricos. Total Recall, con la tecnología subyacente de Flashback Data Archive, realiza un seguimiento transparente de los cambios en las tablas de bases de datos, de forma segura y eficaz, sin necesidad de interfaces especiales o cambios de aplicaciones.

Conclusión

Las soluciones de seguridad transparentes son fundamentales para la economía globalizada de hoy en día, debido a los costos y la complejidad de modificar el código de las aplicaciones existentes. Lograr el cumplimiento normativo y reducir el riesgo de amenazas internas requiere una mayor protección de los datos de las aplicaciones. Los

productos de seguridad de Oracle Database están diseñados para funcionar de forma transparente y reducir el impacto sobre las aplicaciones existentes, a la vez que se satisfacen los requisitos de las diversas reglamentaciones. Los productos de seguridad de Oracle Database ofrecen defensa en profundidad mediante tres capas de seguridad: cifrado y enmascaramiento, control de acceso y monitoreo.

Oracle Advanced Security TDE sigue siendo el sistema de cifrado líder de la industria y ofrece una cómoda solución para proteger la información privada y cumplir con normativas como las establecidas por PCI. Oracle Database 11g introdujo el cifrado de espacios de tablas completos y la integración con módulos de seguridad de hardware, lo que permite el cifrado aplicaciones enteras y el almacenamiento centralizado de las claves maestras de cifrado TDE. Oracle Data Masking permite que los evaluadores, desarrolladores y socios accedan a los mismos datos de producción, pero sólo después de la des-identificación de los datos delicados.

Oracle Database Vault ofrece una respuesta transparente para los exigentes requisitos de control interno de SOX, PCI, HIPAA y otras normativas. Los dominios de Oracle Database Vault impiden que los DBA tengan acceso a información financiera delicada o privada de las aplicaciones. Las etiquetas de clasificación de datos de Oracle Label Security permiten automatizar la aplicación de seguridad de los datos según la confidencialidad de cada fila.

Oracle Enterprise Manager Configuration Management Pack monitorea continuamente los hosts y las bases de datos para detectar infracciones de seguridad y mejores prácticas de seguridad, lo cual simplifica notablemente el trabajo del administrador de seguridad. Oracle Audit Vault transforma los datos de auditoría en un recurso de seguridad clave, al consolidar y proteger de forma transparente la información de auditoría fundamental asociada con la actividad de la base de datos. Los informes, las alertas y las políticas de Oracle Audit Vault agilizan el trabajo del personal de cumplimiento normativo y los encargados de seguridad.

Proteger los datos contra ataques sofisticados es un desafío, pero la tecnología de seguridad de defensa en profundidad de Oracle facilita la tarea gracias a sus soluciones transparentes y de excelente rendimiento.

Seguridad de Oracle Database
Junio de 2009
Autor: Oracle
Colaboradores:

Oracle Corporation
Sede mundial
500 Oracle Parkway
Redwood Shores, CA 94065
EE. UU.

Consultas internacionales:
Teléfono: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com

Oracle is committed to developing practices and products that help protect the environment

Copyright © 2009, Oracle o sus subsidiarias. Todos los derechos reservados. Este documento se proporciona exclusivamente con fines informativos y sus contenidos están sujetos a cambio sin previo aviso. No se garantiza que el presente documento esté libre de errores, ni tampoco está sujeto a otras garantías y condiciones, ya sean expresadas oralmente o implícitas en la legislación, incluidas garantías y condiciones implícitas de comerciabilidad o adecuación para un propósito en particular. Oracle se exime específicamente de cualquier responsabilidad respecto del presente documento y tampoco se establece relación contractual directa o indirecta alguna mediante el mismo. El presente documento no podrá reproducirse, ni transmitirse de forma ni por medio alguno, sea éste electrónico o mecánico, para finalidad alguna, sin el expreso consentimiento escrito de Oracle Corporation.

Oracle es una marca comercial registrada de Oracle Corporation y/o sus subsidiarias. Los demás nombres pueden ser marcas comerciales de sus respectivos propietarios.

0109