



Hedgehog vPatch™

Parches Virtuales para Proteger Bases de Datos



Hedgehog vPatch de Sentrigo reduce significativamente el riesgo de intrusión y robo de información en bases de datos. El mismo ofrece protección a la Base de Datos en tiempo real frente a ataques de vulnerabilidades conocidas, tales como inyecciones SQL y ataques de buffer overflow. Hedgehog vPatch protege la BD sin requerir bajar la misma y sin testear aplicaciones.



Hedgehog vPatch dashboard

Ventajas del Producto

- Protección en tiempo real de la BD ante vulnerabilidades conocidas
- No es necesario bajar la BD. Posee cero impacto sobre las aplicaciones, tanto durante la instalación como durante las actualizaciones
- Software escalable y fácil de implementar
- Reduce significativamente el riesgo de ataques durante instalaciones de parches del vendedor de la BD
- La única forma de proteger a versiones de BD no soportadas por los fabricantes

La solución de Sentrigo protege los datos sensibles a través de:

- Cubriendo y protegiendo las BD de los riesgos existentes de vulnerabilidades no parchadas aun
- Detectando y previniendo en tiempo real de intentos de ataque e intrusiones
- Optimizando el proceso de parcheado y reduciendo la sobrecarga
- Endureciendo virtualmente la BD para rectificar una configuración débil

Descargue la versión gratuita de evaluación de Hedgehog Enterprise desde nuestro sitio web:

www.virtual-patching.com



Hedgehog vPatch™

Parches Virtuales para Proteger Bases de Datos

Insider Threat

Auditing

SQL Injection

Privacy

SAS 70

Monitoring

Virtual Patching

Sarbanes-Oxley

Breach Prevention

PCI DSS

HIPAA

Hedgehog vPatch crea un nivel de seguridad extra alrededor de la Base de Datos y la cubre y protege de vulnerabilidades

Las Bases de Datos son Vulnerables

La complejidad de las bases de datos las hace susceptibles a distintos tipos de vulnerabilidades de seguridad que proveen un punto de entrada para intrusos y usuarios no autorizados. Hay cientos de vulnerabilidades desconocidas, entre las cuales las mas severas permiten acceso remoto a usuarios no autenticados, resultando en ataques que pueden afectar seriamente la organización o facilitar el robo a gran escala. Mientras los fabricantes de BD parchan regularmente sus productos, la realidad es que la aplicación de dichos parches es una tarea dificultosa requiriendo generalmente el testeo intensivo de aplicaciones. Debido a esa complejidad, muchas empresas no parchan sus bases de datos tan frecuentemente como deberían, y en algunos casos no lo hacen nunca.

Los Parches Virtuales llenan el vacio

La dificultad de mantener las bases de datos de la organización parchadas, y el constante cambio en el terreno de las vulnerabilidades, requieren una nueva forma de aproximación. Los Parches Virtuales protegen la BD de ataques sin parchar el kernel de la misma. Crean un nivel extra de seguridad sobre la base de datos que a diferencia de los parches de los fabricantes, no requieren bajara o testear las aplicaciones. A través del monitoreo de todas las acciones en la Base de Datos y el chequeo de la mismas contra reglas de exploits y vulnerabilidades conocidas, los parches virtuales detectan dichos intentos maliciosos. Cuando ello ocurre, una alerta es emitida y la sesión sospechosa puede ser terminada y la aplicación de origen o el usuario, pueden ser puestos e cuarentena por un periodo especificado hasta que la naturaleza del ataque sea investigada.

vPatch de Hedgehog es la Solución

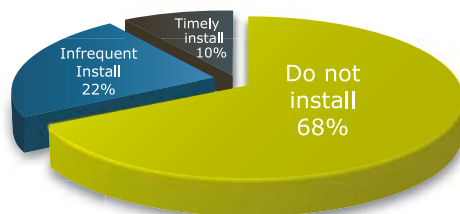
Hedgehog vPatch en una solución basada software que se provee por medio de una suscripción, y protege las bases de datos en tiempo real ante vulnerabilidades conocidas utilizando las cualidades únicas del producto. La misma emplea agentes de software para proteger la BD con un grupo de parches virtuales protectivos para detectar y prevenir intentos de explotar las vulnerabilidades conocidas en la BD. El equipo Rojo de Sentrigo compuesto de investigadores en seguridad informática continuamente estudia las vulnerabilidades en las bases de datos con el fin de encontrar formas de detenerlas. El equipo tiene como objetivo proveer, dentro de un periodo corto de tiempo ,una regla (parche virtual) para cada vulnerabilidad previamente conocida. No es necesario detener ni bajar la base de datos durante la instalación del producto, ni tampoco durante la actualización y de los vPatches.

Tomando un Gran Riesgo

La Encuesta de Sentrigo sobre Parcheo en Bases de Datos

Sentrigo publica una encuesta basada en 300 profesionales de Oracle, donde se revela que dos tercios de los usuarios respondieron que nunca aplicaron los parches trimestrales. Además de ello los encuestados reportan que el proceso de parchado consume mucho tiempo, y requiere regularmente detener y bajar la Base de Datos, al igual que el testeo y regresión de todas las aplicaciones.

Oracle CPU Installations



Sentrigo CPU Survey (January 2008)

Requerimientos del Sistema

Hedgehog IDentifier es una agregado a Hedgehog Enterprise.

Servidores de Aplicacion:

JavaEE (IBM WebSphere, BEA WebLogic, Apache Tomcat, JBoss, etc.) o Microsoft .NET

Informacion de Contacto

Sentrigo, Inc. 155M New Boston St. Suite 130 Woburn, MA 01801 USA

Tel: 781.935.2984 info@sentrigo.com

Capacidades de Producto

- Actualizaciones continuas y frecuentes de defensas ante ataques
- Fácil implementación de las actualizaciones
- Facilita el cumplimiento de normativas teniendo los sistemas actualizados
- No son necesarias las customizaciones ni el conocimiento específico sobre las BD
- Se instala en minutos y es escalable a lo largo de la organización

Descargue la versión gratuita de evaluación de Hedgehog Enterprise desde nuestro sitio web:

www.sentrigo.com