

Ley de Protección de Datos Personales

Monitoreo de Actividad de Base de Datos

Ing. Marcelo Guelfi
Security Advisor

¿Por qué DAM?

- Las Bases de Datos se han convertido en las 'Joyas de la Corona'...



¿Por qué DAM?

- No siempre las protegemos en relación a su valor...
- Y al tipo de ataques...



Principales motivos de DAM

■ Cumplimiento de regulaciones

- Ley N° 18331 de Protección de Datos Personales
- Crecimiento de regulaciones y estándares como SOX y PCI DSS.

■ Controles de Seguridad

- Alto volumen de robo de datos tanto interno como externo.

■ Mayor exposición de las bases de datos

- Cambio de acceso por terminales a navegadores que pueden correr desde un celular que se conecta via VPN-SSL.
- Aplicaciones de terceros.
- Usuarios genéricos

Características de DAM

- Habilidad para monitorear y auditar en forma independiente toda la actividad de una base de datos, incluidas las realizadas por un DBA y las consultas.
- Almacenar esta actividad fuera de la base en forma segura.
- Realizar la separación de tareas: el que administra no audita.
- Generar alertas en caso de violaciones de seguridad o actividad inusual.
- Generar Reportes de cumplimiento de normas.

Características avanzadas

- Herramienta integrada de evaluación de vulnerabilidades.
- Creación de perfiles dinámicos basados en el acceso a la base.
- Detección de cambios de comportamientos por parte de los usuarios.
- Detener las operaciones antes de que se ejecuten en la base de datos.
- Poner usuarios/terminales en cuarentena hasta que se resuelva el incidente.
- Establecer límites en la cantidad de registros por consulta y disparar una alerta en caso de que se supere.
- Detectar patrones correspondientes a datos confidenciales (si en el resultado van nombres + números de tarjeta).
- Almacenar los cambios realizados en los datos sensibles (antes y después).

Alternativas de seguridad en DB

- Auditoría Nativa
 - Viene con la base de datos.
 - No ofrece separación de roles.
 - Impacto en el rendimiento cuando se habilita en forma completa.
 - Depende de cada RDBMS.

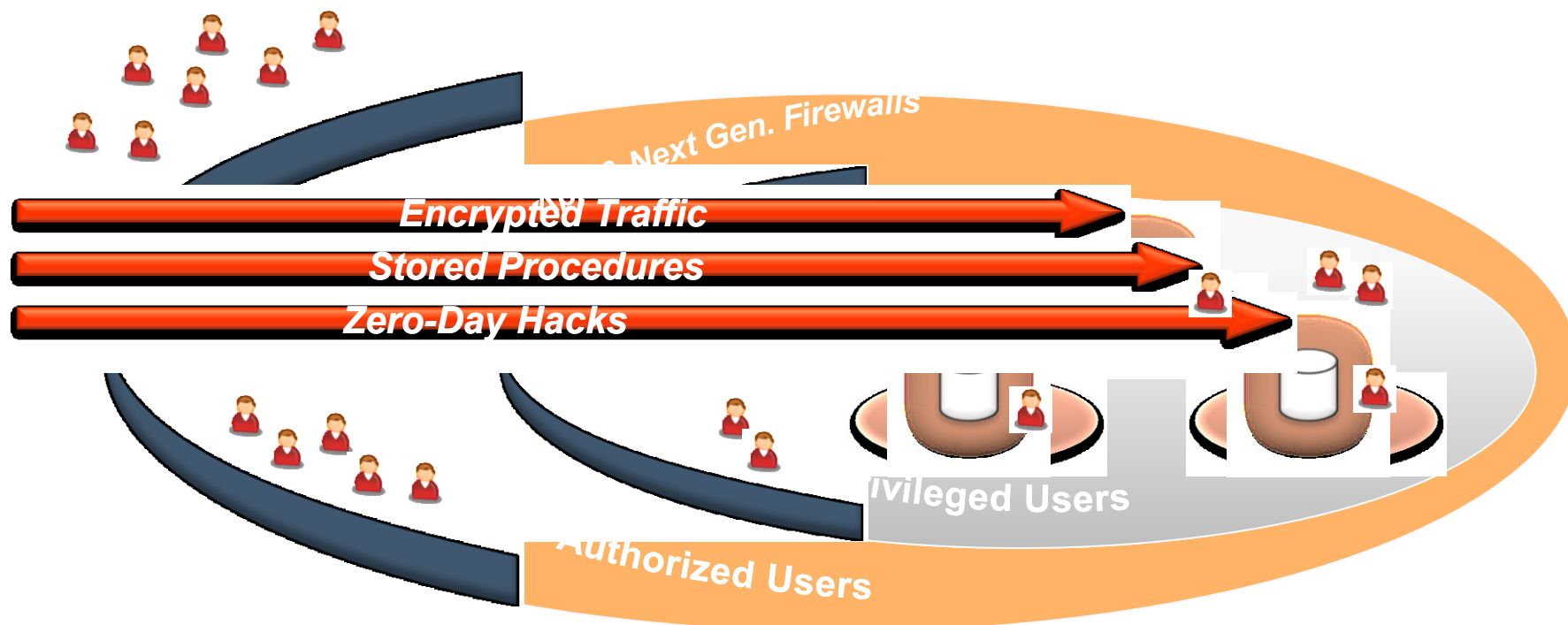
- Opciones de Bridge (hardware) o port mirroring (hardware o software)
 - No es invasivo.
 - No afecta el rendimiento de los servidores de DB.
 - Independiente del fabricante y versiones de la base.
 - Repositorio central para controlar más de una base de datos.
 - No puede controlar accesos locales (ssh, VNC, etc).

- Agentes en el servidor
 - Visibilidad total de todos los protocolos y usuarios.
 - Utiliza recursos del servidor pero no supera el 5 o 10% de un procesador.

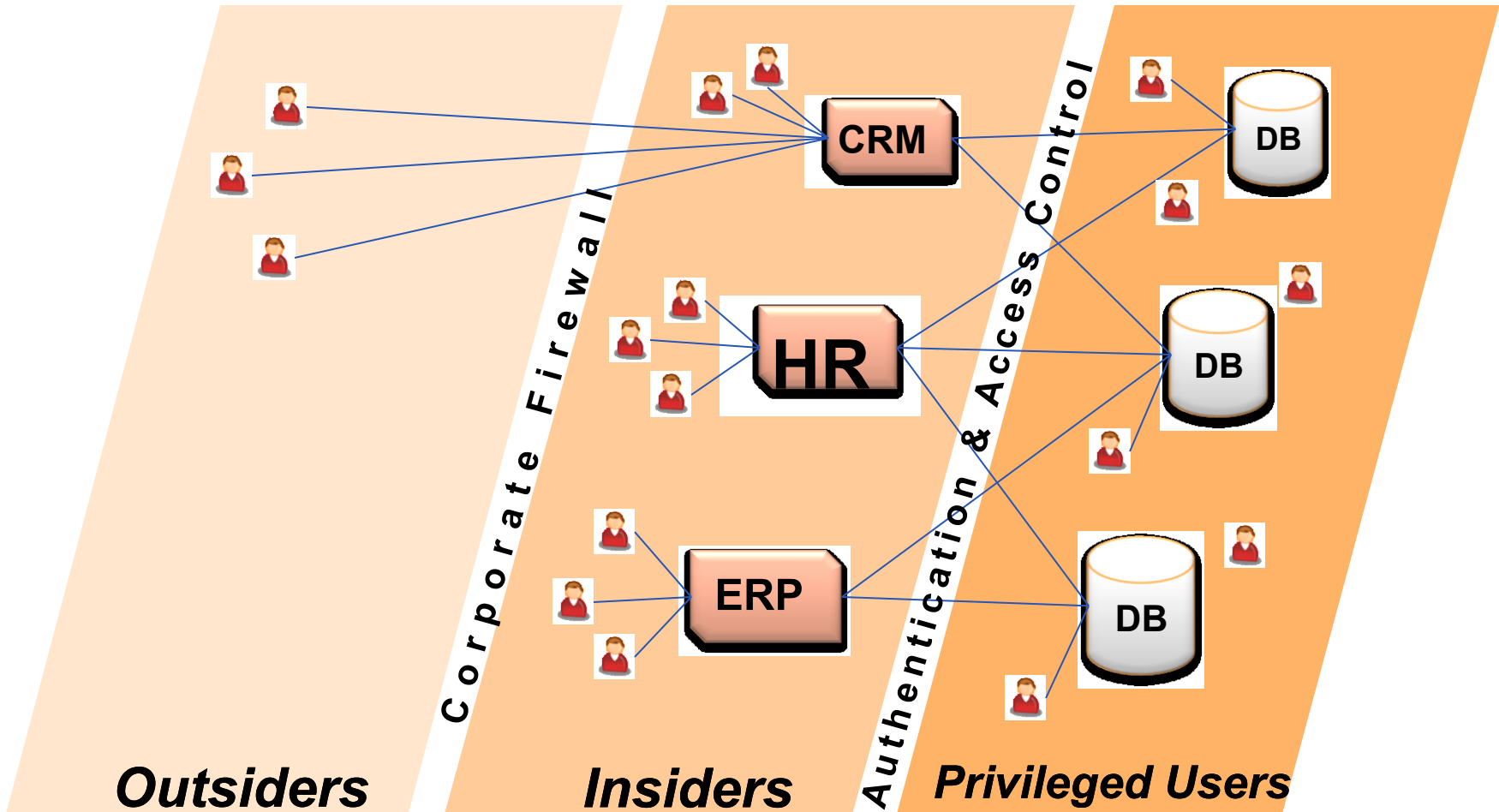
- Combinación de los anteriores

La complejidad del problema

Las bases de datos siguen vulnerables a ataques externos...
y a más violaciones internas de usuarios privilegiados...
las aplicaciones web de firewalls proporcionar protección limitada...



Estructura actual de seguridad



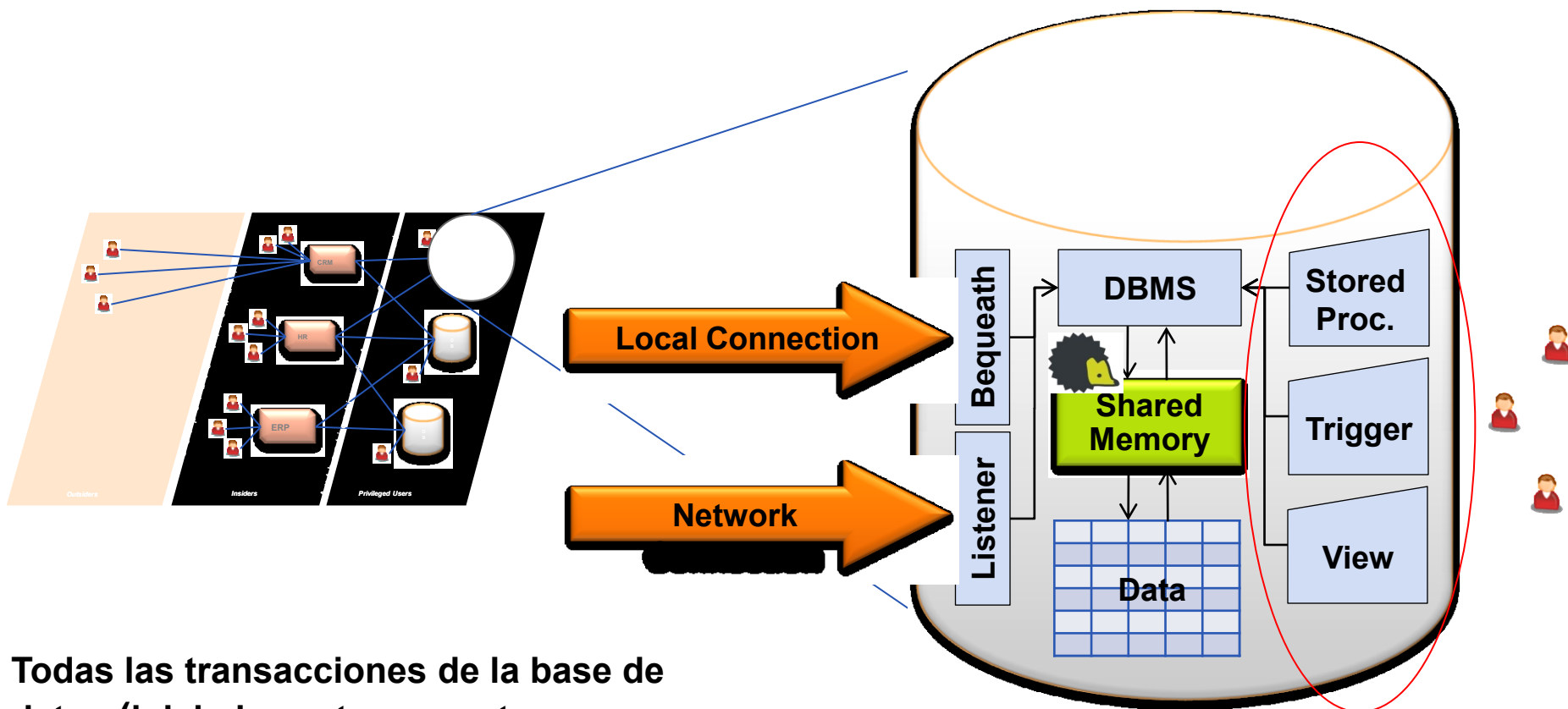
Propuesta: complemento a la seguridad perimetral

- La protección se establece desde el interior.
- Estudio inicial de vulnerabilidades.
- Buenas prácticas

Ejemplo de una solución

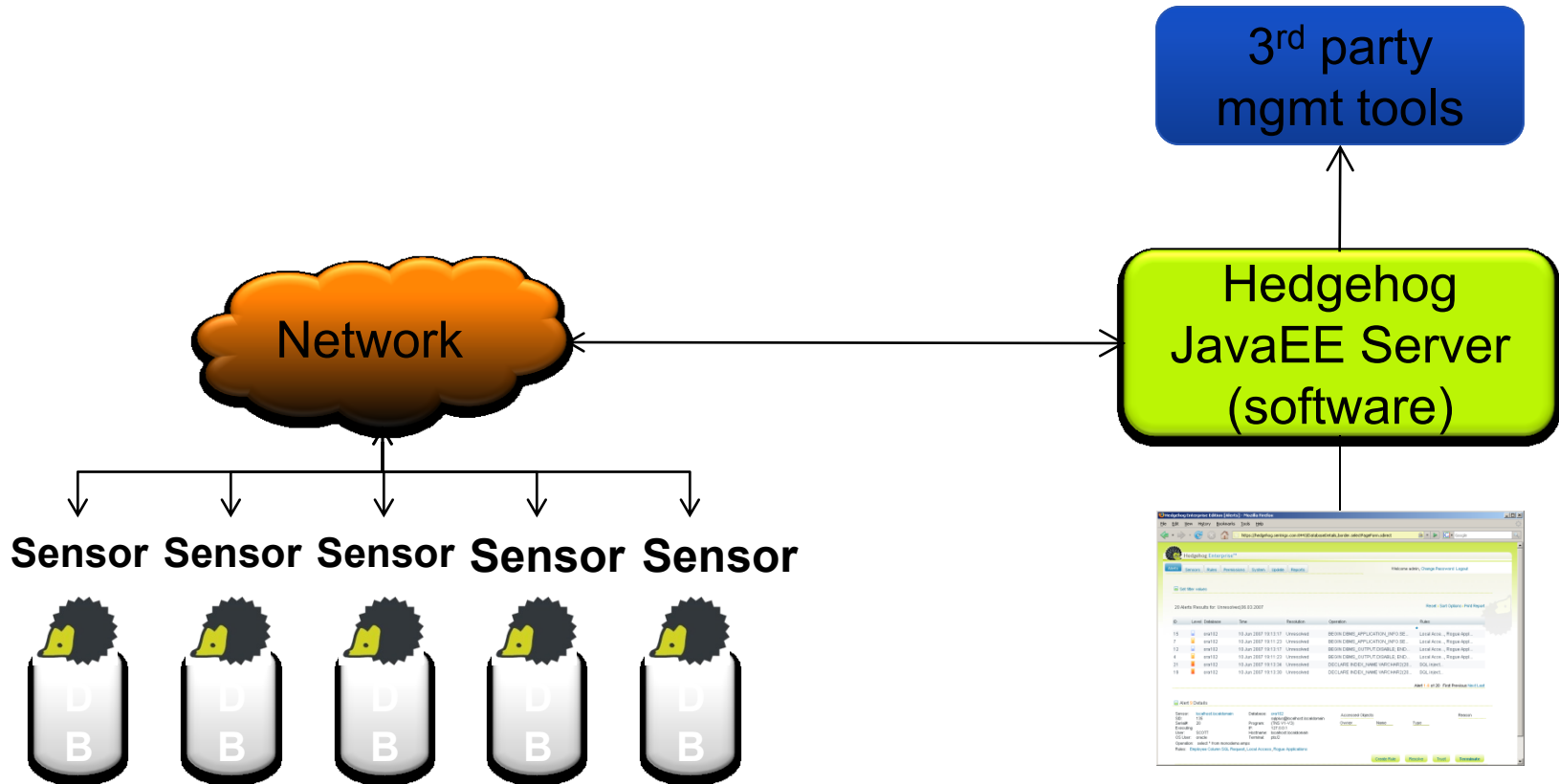
- HedgeHog Enterprise.
- HedgeHog Identifier.
- HedHog vPatch.

HedgeHog Enterprise



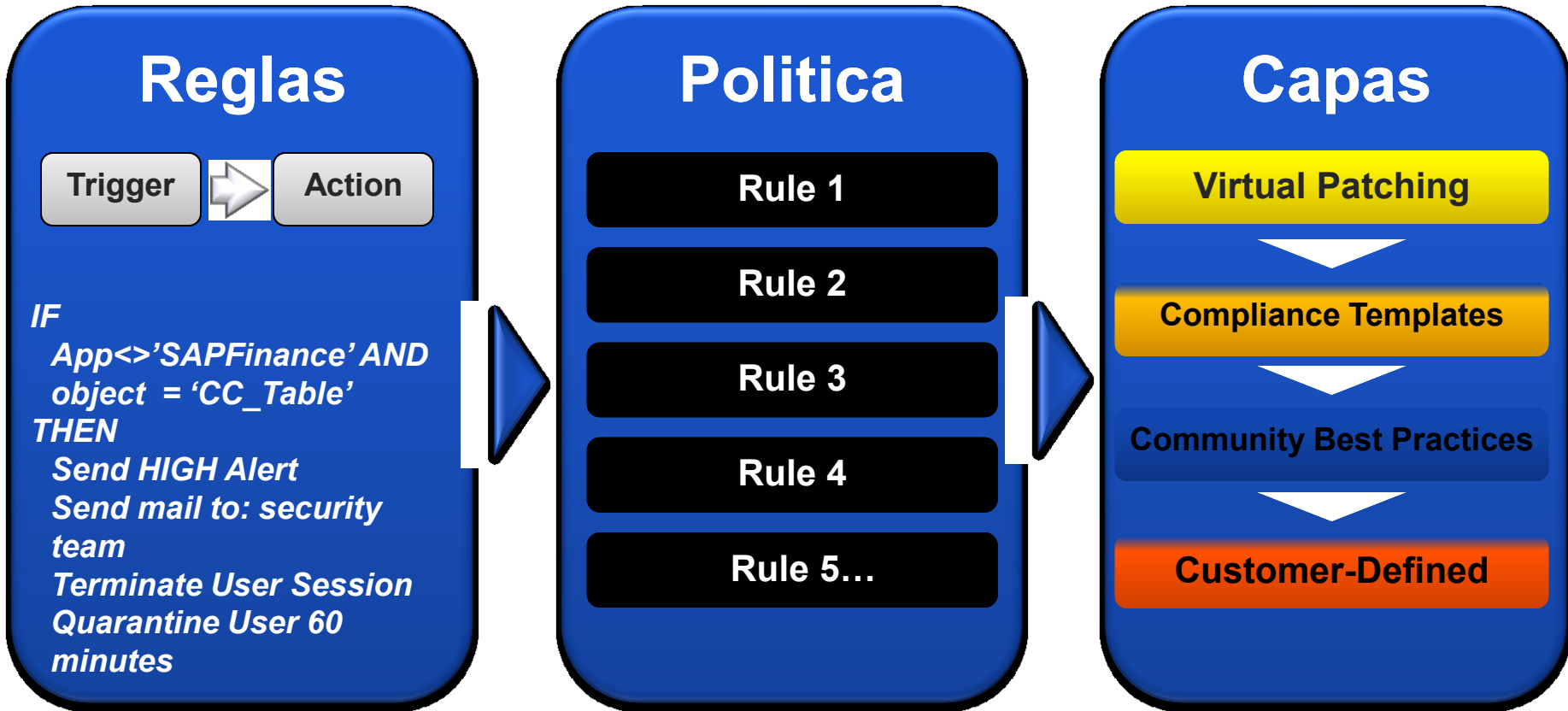
Todas las transacciones de la base de datos (iniciadas externamente-o internamente) pasan por la memoria compartida

Visión general de la estructura



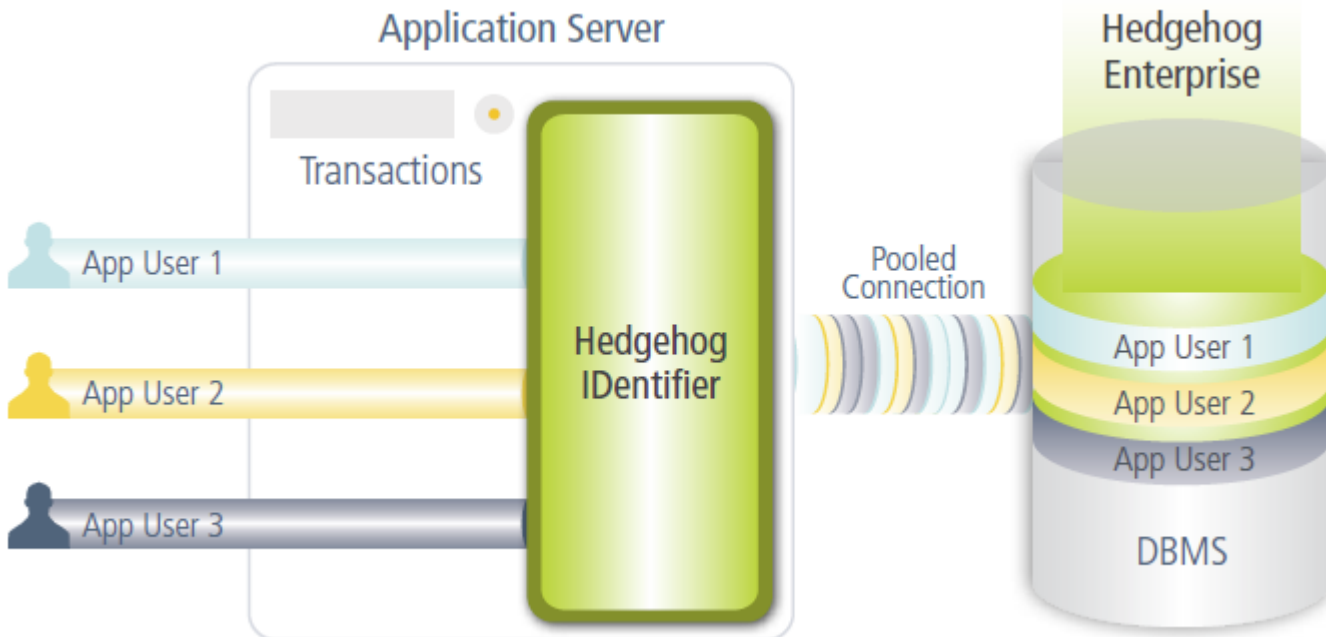
Web-based
Admin Console

Cómo trabaja



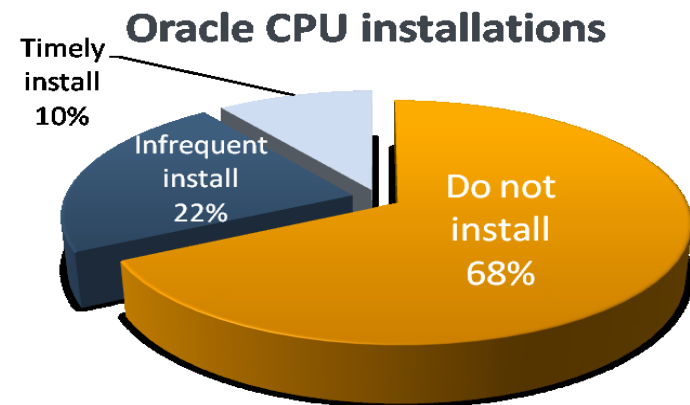
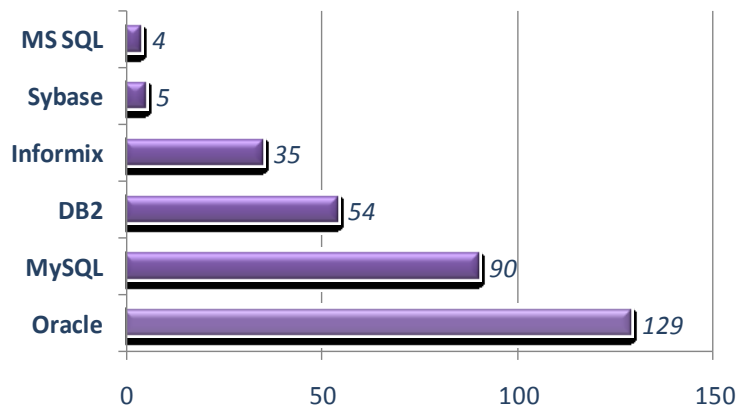
Hedgehog Identifier

- Permite identificar los accesos que se hacen desde pooles de conexiones.
- Funciona con servidores de aplicaciones J2EE y .NET



Vpatch – Protección virtual

- Más de 100 vulnerabilidades severas abiertas en todo momento.
- Los usuarios no aplican los parches:
 - Los creadores de las aplicaciones suelen aconsejar no instalar los parches.
 - DB debe estar offline y debe hacerse un test para validar que todo funcione



Vulnerabilidades - vpatch



- Exploits publicados en la web
 - Zero-days (antes del parche)
 - Dentro de los días que el parche se publica
 - No requieren el nivel de habilidad de un DBA
- La ventana de riesgo es de meses o a veces de años
- El riesgo crece después de que el parche se publica

Preguntas

