

# Hedgehog vPatch™

## Virtual Patching for Database Protection



Hedgehog vPatch verringert signifikant die Risiken, die durch Einbruchsversuche in die Datenbank oder durch Datendiebstahl entstehen. Das DBMS wird in Echtzeit vor dem Ausnutzen bekannter Sicherheitslücken, wie SQL-Injection und Buffer Overflow bewahrt. Hedgehog vPatch schützt die Datenbank und erfordert weder eine Downtime noch das Testen von Applikationen.

### Produkt Highlights

- Echtzeit-Schutz des DBMS gegen bekannte Sicherheitslücken
- Keine Downtime und kein Einfluß auf die Applikationen während Installation und Update
- Skalierbar, einfache Softwareverteilung
- Signifikante Risikominimierung für die Zeitspanne zwischen Veröffentlichung und Installation von Hersteller-Patches
- Die einzige Möglichkeit zum Schutz von DBMS-Versionen, für die der hersteller keine Updates mehr liefert



Sentrigos Hedgehog schützt sensible Daten durch:

- Abschirmung der Datenbanken vor dem Risiko, das von ungepatchten Sicherheitslücken ausgeht
- Erkennung und Abwehr von Eindringversuchen und Angriffen in Echtzeit
- Optimierung des Patchverfahrens und Reduzierung von Overhead
- Virtuelles Härten der Datenbank als Mittel gegen schwache Konfigurationen

Download: Kostenlose Testversion  
 von Hedgehog vPatch:  
[www.virtual-patching.com](http://www.virtual-patching.com)

# Hedgehog vPatch™

## Virtual Patching for Database Protection



Hedgehog vPatch legt eine Sicherheitsschicht um die Datenbank zum Schutz gegen Angriffe

### Datenbanken sind verwundbar

Die Komplexität von Datenbanken macht sie anfällig für viele Sicherheitslücken, die als Hebel für Angreifer und unberechtigte Anwender dienen. Es gibt Hunderte von bekannten Sicherheitslücken. Die gefährlicheren unter ihnen erlauben Remote-Zugriff durch nicht autorisierte User und können ernsthaft das Unternehmen lahmlegen, oder die Gelegenheit zu massivem Datendiebstahl bieten.

Während Datenbankhersteller darauf achten, regelmäßig DBMS-Patches herauszugeben, ist in Wirklichkeit dieses Patchen eine sehr schwierige Aufgabe, die normalerweise Downtime für die Datenbank bedeutet und ausführliches Testen der Anwendungen erfordert. Auf Grund dieser Hürden verzichten viele Unternehmen darauf, die Datenbanken im erforderlichen Maße zu patchen.

### Virtuelles Patchen schließt die Lücke

Die Schwierigkeit den Patchlevel wichtiger Datenbanken aktuell zu halten und die ständige Änderungen von Bedrohungsszenarien erfordert eine neue Herangehensweise. Virtuelles Patchen schützt die Datenbank vor Angriffen, ohne aktuelles Patchen des DBMS-Kerns. Es wird eine Sicherheitsschicht um die Datenbank gelegt, die anders als beim Einspielen der Hersteller-Patches, weder Downtime noch Testen von Applikationen erfordert.

Durch Überwachen aller Datenbankaktionen und deren Überprüfung durch Regeln, die Angriffe und Schwachstellen erkennen, identifiziert Virtuelles Patchen Angriffsversuche. Bei Regelverletzung wird ein Alarm erzeugt und die verdächtige Session kann beendet werden. Der Verursacher (User, Anwendung) kann für eine bestimmte Zeit in Quarantäne gestellt werden, während die verdächtige Aktion untersucht wird.

### Hedgehog vPatch ist die Lösung

Hedgehog vPatch ist eine host-basierte Software, ausgeliefert als Abo, die durch ihre einzigartigen Fähigkeiten die Datenbanken in Echtzeit gegen unbekannte Schwachstellen schützt. vPatch verwendet Software-Agenten zum Schutz des DBMS, ausgestattet mit einem Satz von virtuellen Patches, die das Ausnutzen von DBMS-Schwachstellen entdecken und verhindern.

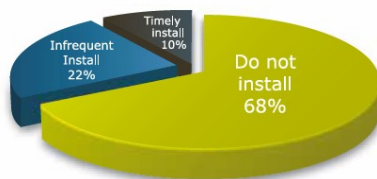
Die Sicherheitsforscher im Red Team von Sentrigo untersuchen laufend Schwachstellen in der Datenbank, um diese abzusichern. Sie analysieren Angriffe gegen die Datenbank mit dem Ziel, Wege zu finden, diese zu verhindern. Das Team strebt danach, vPatch-Regeln für jede nicht geschützte Schwachstelle innerhalb kürzester Zeit zur Verfügung zu stellen. Eine Downtime ist weder für die Erstinstallation, noch für die laufende Verteilung der aktualisierten vPatche erforderlich.

### Ein großes Risiko

#### Die Sentrigo Umfrage: „Patchen von Datenbanken“

Sentrigo veröffentlichte eine Umfrage von über 300 Oracle-Experten, die aufzeigt, daß zwei Drittel der befragten User nie einen der vierteljährlich erscheinenden Patches eingespielt haben. Als Gründe wurde genannt, daß das Einspielen der Patches zu zeitaufwändig sei und in der Regel eine Downtime der Datenbank sowie ein Regressionstest der Anwendungen erforderlich wäre.

Oracle CPU Installations



Sentrigo CPU Survey (January 2008)

- Automatische und häufige Aktualisierungen der Abwehrmaßnahmen gegen Angriffe
- Verteilung der aktualisierten virtuellen Patche auf Knopfdruck
- Unterstützung der Compliance indem das System "up to date" gehalten wird
- Keine Anpassungen oder DBMSspezifisches Wissen erforderlich

### Systemanforderungen

#### Überwachte Datenbank – Hedgehog Sensor:

Oracle 8.1.7 oder besser unter Sun Solaris, IBM AIX, Linux, HP-UX, Windows Microsoft SQL Server unter Windows

#### Hedgehog Server:

Sun Solaris, Linux oder Windows OS 1 GB (512 MB frei) RAM 1 GB freier Plattenplatz

#### Hedgehog Management Konsole:

Mozilla Firefox 1.5 oder besser, Microsoft Internet Explorer 6.0 oder besser

#### Kontakt

Sentrigo, Inc., 155M New Boston St., Suite 130, Woburn, MA 01801 USA  
 The Bristol Group, 63255 Langen, 06103-2055-300, [www.bristol.de](http://www.bristol.de)

Download: Kostenlose Testversion  
 von Hedgehog vPatch:

[www.virtual-patching.com](http://www.virtual-patching.com)