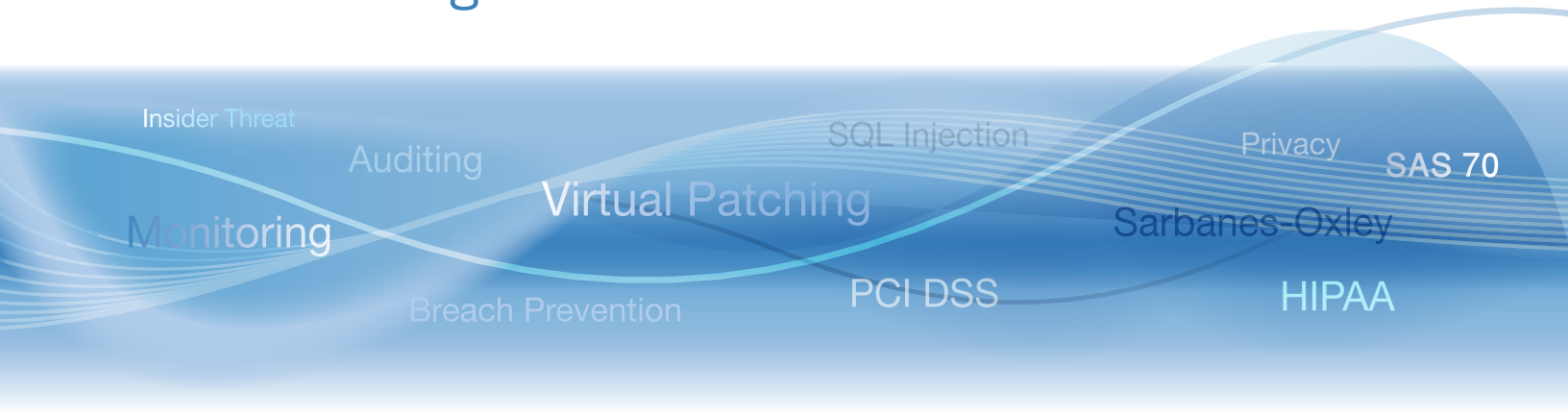
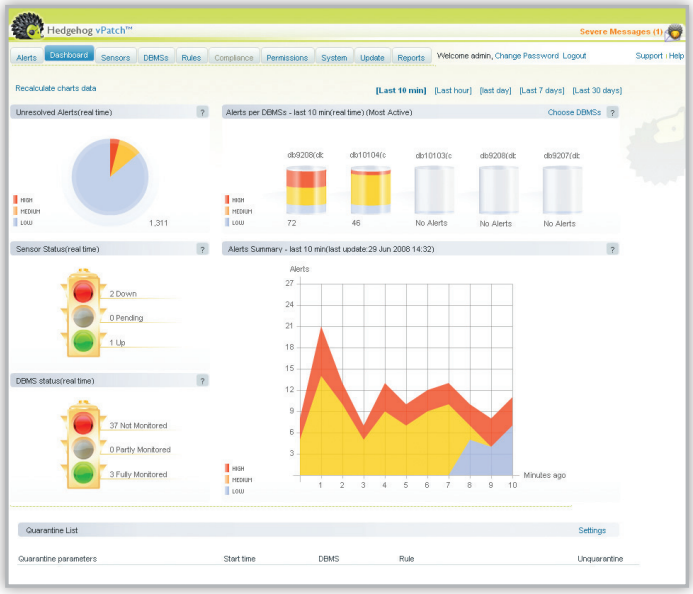
Hedgehog vPatch™

Virtual Patching for Database Protection



Sentrigo's Hedgehog vPatch significantly reduces the risk of database intrusion and data theft. It offers real-time DBMS protection against exploits of known vulnerabilities, such as SQL injection and buffer overflow attacks. Hedgehog vPatch shields the database without requiring database downtime or application testing.



Hedgehog vPatch dashboard

Product Highlights

- Real-time protection of the DBMS from known vulnerabilities
- No downtime and zero impact on applications both during installation and updates
- Scalable and easy to deploy software
- Significantly reduces the risk between vendor patch installations
- The only way to protect DBMS versions no longer supported by vendors

Sentrigo's Hedgehog solution protects sensitive data by:

- **Shielding databases from** the risk presented by unpatched vulnerabilities
- **Detecting and preventing** attempted attacks and intrusions in real time
- **Optimizing** the patching process and reduce overhead
- **Virtually hardening** the database to rectify weak configuration

Download a free trial version of Hedgehog vPatch from:

www.virtual-patching.com

Hedgehog vPatch™

Virtual Patching for Database Protection

Hedgehog vPatch creates a security layer around the database and shields it from exploits

Databases Are Vulnerable

The complexity of databases makes them susceptible to many security vulnerabilities that provide an entry point for intruders and unauthorized users. There are hundreds of known vulnerabilities, the more severe among them allowing remote access by unauthenticated users, and resulting in attacks that can seriously cripple the enterprise or facilitate large-scale data theft.

While database vendors are on guard to issue DBMS patches on a regular basis, the reality is that patching databases is a difficult task, usually requiring database downtime and extensive application regression testing. Due to these hurdles, many enterprises do not patch their database as frequently as they should, and in some cases, not at all.

Virtual Patching Fills the Gap

The difficulty of keeping enterprise databases patched, and the constantly changing threat landscape require a new approach. Virtual patching protects the database against exploits without actually patching the DBMS kernel. It creates a security layer around the database that, unlike vendor patching, does not require downtime or application testing.

By monitoring all actions in the database and matching them against rules that detect known exploits and vulnerabilities, virtual patching detects attempted exploits. When a match occurs, an alert is issued and the suspicious session can be terminated and the originating application or user quarantined for a specified period, until the nature of the suspected attack is investigated.

Hedgehog vPatch Is the Solution

Hedgehog vPatch is a host-based software, provided by subscription, that protects databases in real-time against known vulnerabilities using unique virtual patching capabilities. It employs software agents to protect the DBMS with a set of protective virtual patches to detect and prevent attempted exploits of DBMS vulnerabilities.

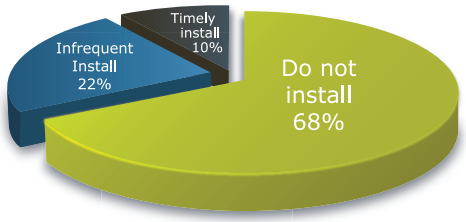
The Sentrigo Red Team of security researchers continually explores database vulnerabilities and exploits in an effort to devise ways of stopping them. The Team strives to provide a vPatch rule for each previously uncovered vulnerability within a short period of time. No database downtime is required both during the initial installation, as well as during the ongoing deployment of updated vPatches.

Taking a Big Risk

The Sentrigo DBMS Patching Survey

Sentrigo published a survey of over 300 Oracle professionals, revealing that two-thirds of users polled had never applied quarterly patches. Respondents reported that the patching process was time-consuming, and regularly required DBMS downtime and the regression testing of appliances.

Oracle CPU Installations



Sentrigo CPU Survey (January 2008)

Features

- Ongoing, frequent updates of defenses against exploits
- Push-button deployment of updated virtual patches
- Facilitates compliance by keeping systems up to date
- No customization or DBMS-specific knowledge required
- Installs in minutes, scalable across the enterprise

System Requirements

Monitored Databases – Hedgehog Sensor:
Oracle version 8.1.7 or later, running on Sun Solaris, IBM AIX, Linux, HP-UX or Windows Microsoft SQL Server on Windows

Hedgehog Server:
Sun Solaris, LINUX or Windows OS 1GB (512MB free) RAM 1GB free disk space

Hedgehog Management Console:
Mozilla Firefox 1.5 or later/MS Internet Explorer 6.0 or later

Contact Information

Sentrigo, Inc., 155M New Boston St., Suite 130, Woburn, MA 01801, USA
Tel: 781.935.2984/2979 info@sentrigo.com

Download a free trial version of Hedgehog vPatch from www.virtual-patching.com.

www.sentrigo.com