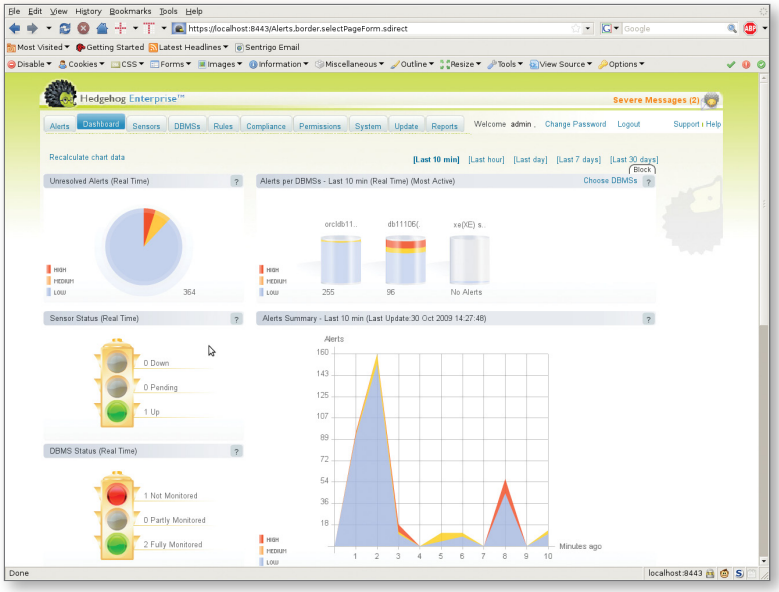
sentrigo™

Hedgehog vPatch™

Virtual Patching for Database Protection

Sentrigo's Hedgehog vPatch significantly reduces the risk of database intrusion and data theft.

Sentrigo's Hedgehog vPatch significantly reduces the risk of database intrusion and data theft by offering 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, providing a greater level of security until vendor patches can be applied.



The Hedgehog vPatch dashboard provides an overview of database security alerts and monitoring status.

Product Highlights

- Real-time protection of the DBMS from known vulnerabilities addressed by vendor patches
- Additional layer of security for common zero-day threat vectors
- No downtime and zero impact on applications both during installation and updates
- Significantly reduces the risk between vendor patch availability and installation
- The only way to protect DBMS versions no longer supported by vendors
- Scalable and easy to deploy software

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 reducing overhead of patch management
- Virtually hardening the database to rectify a weak configuration and meet compliance requirements

Download a free Trial of Hedgehog vPatch:
www.sentrigo.com

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, the suspicious session can be terminated, and the originating user can be quarantined for a specified period, allowing timer for the suspected attack to be investigated.

Hedgehog vPatch Is the Solution

Hedgehog vPatch is host-based software, provided by subscription, that protects databases in real-time against known vulnerabilities using unique virtual patching capabilities. It employs memory-based sensors to protect the DBMS with a set of 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. Soon after each vendor patch is released, the Red Team updates the vPatch rules with protection for newly discovered vulnerabilities. No database downtime is required both during the initial installation, nor for the ongoing deployment of updated vPatches.

Key Features

- Real-time alerts delivered to the Hedgehog dashboard, e-mail or to any SIEM or system management tool via SNMP, SysLog, or direct integration
- Ongoing, frequent updates of defenses against exploits
- Push-button deployment of updated virtual patches to all affected systems
- 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, Microsoft Windows

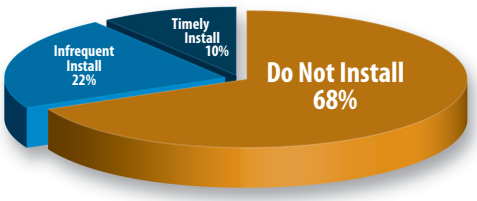
Microsoft SQL Server 2000, 2005, or 2008 on any supported Windows platform

Sybase ASE 12.5 on all supported platforms

Hedgehog Server:
Sun Solaris, LINUX or Windows OS, with 2 GB RAM and 1GB free disk space

Hedgehog Management Console:
Mozilla Firefox 2.0 or later / MS Internet Explorer 7.0 or later

Taking a Big Risk: The Sentrigo DBMS Patching Survey



ORACLE CPU INSTALLATIONS

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.

sentrigo™

Sentrigo, Inc.
2620 Augustine Drive,
Suite 145
Santa Clara, CA 95054
USA Tel: 408.970.3300
info@sentrigo.com

VP-DS-060410-01