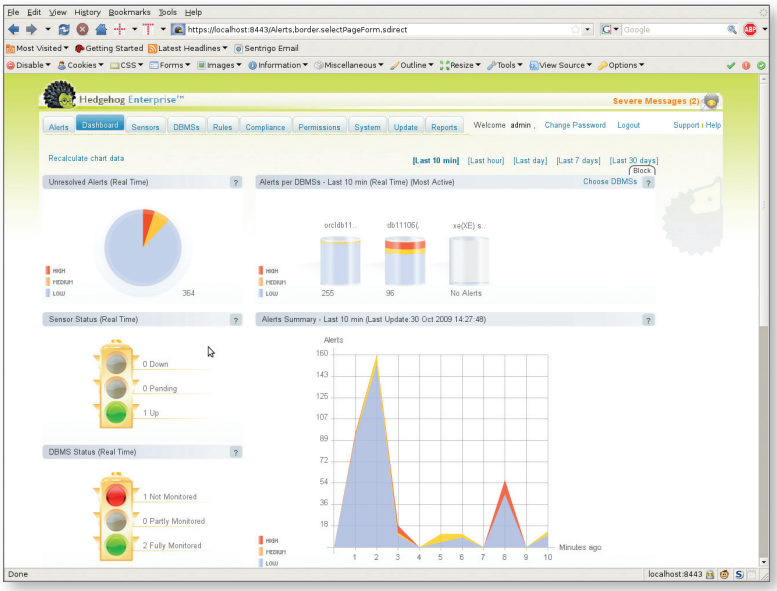
sentrigo™

Hedgehog Enterprise™

Database Activity Monitoring and Intrusion Prevention

Maximum protection for sensitive data, quickly meeting compliance requirements and reducing exposure to a costly breach.

Sentrigo's Hedgehog Enterprise is a host-based, software-only, scalable database activity monitoring and intrusion prevention solution, providing full visibility into all database activity, including local privileged access. By protecting the database in real-time with actionable alerts and prevention capabilities, Hedgehog Enterprise allows organizations to enforce security policy and comply with regulatory requirements, such as PCI DSS, Sarbanes-Oxley, SAS 70 and HIPAA.



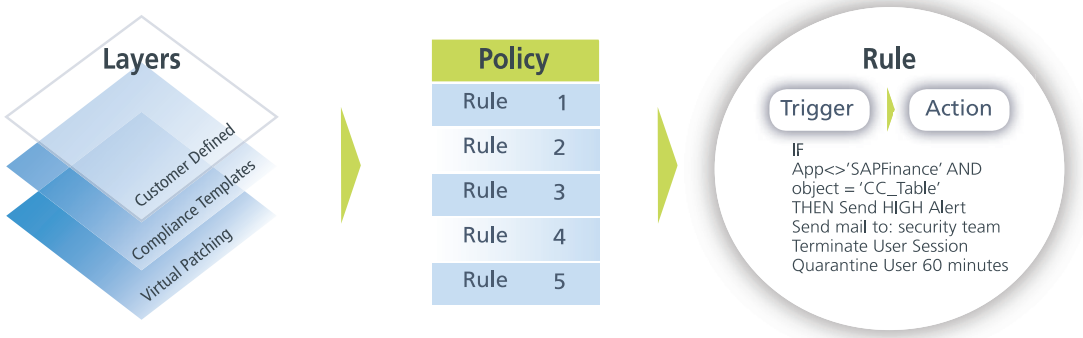
The Hedgehog Enterprise dashboard provides an overview of database security alerts and monitoring status.

Product Highlights

- Real-time alerting and prevention of attacks from external threats or privileged insiders
- Wizard-driven templates to meet compliance requirements
- Automatically discovers databases on the network and organizes them for monitoring and management
- Application Mapping collects database usage statistics to assist in creating custom policies
- Granular protection of sensitive data at the object level, regardless of the source of the attack
- Virtual patching that addresses known DBMS vulnerabilities and common threat vectors
- Central management for deployments from a single database to thousands of databases
- Minimal impact on database performance
- Supports Virtualization and Cloud Computing
- Integrated with Sentrigo's full suite of database security products for vulnerability assessment, auditing, and end-user accountability
- Software-only solution, easy to download, install, and deploy

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

Sentrigo's inside-out approach to database security provides the ONLY solution that sees ALL security threats, acts on them on real-time and meets your compliance requirements in the most efficient way.



Hedgehog provides layers of security starting with out-of-the-box protection through compliance-driven rules to granular, highly customized policies.

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 or 15 on all supported platforms

Hedgehog Server:
Sun Solaris, LINUX or Windows OS, with 2 GB RAM

Hedgehog Management Console:
Mozilla Firefox 2.0 or later
MS Internet Explorer 7.0 or later
Google Chrome 6.0 or later

To best meet compliance requirements, you need to protect from ALL threats

Attacks targeting valuable data stored in databases can come from anywhere:

- across the network or via applications
- from local users connected to the server directly
- from inside the database itself, using stored procedures. triggers or views

Hedgehog uses memory-based sensors to catch all three types of threats with a single, non-intrusive solution to demonstrate compliance.

A distributed, software-only solution is faster to deploy and more efficient

By truly distributing the responsibility for implementing security policy to autonomous sensors running on each database server, Hedgehog can be implemented without native auditing, and with no special hardware or additional servers. Hedgehog can be implemented and begin protecting databases in under an hour, automatically scanning the network for databases and quickly building a custom security policy.

Identifies threats as they occur, and intervenes to stop attacks

Unlike basic auditing or log analysis which can only tell you what happened after the fact, Hedgehog stops breaches before they cause damage. Alerts are sent directly to the monitoring dashboard with full details of the policy violation for remediation purposes. High risk violations can be configured to automatically terminate suspicious sessions and quarantine malicious users, allowing time for the security team to investigate the intrusion.

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
- Protects sensitive data by terminating activity based on policy violations, and quarantining users with suspicious activity
- Out-of-the-box protection against known vulnerabilities, including SQL injection, buffer overflow, and privilege escalation attacks
- Detects and blocks intra-database threats based on stored procedures, triggers and views
- Monitors databases in virtualized environments, including data access from VM to VM running on the same physical machine
- Efficiently supports remote sensors in the cloud over WAN connections, by minimizing and compressing traffic between the sensor and server
- Provides flexible reporting, including pre-configured templates for PCI-DSS, Sarbanes-Oxley, HIPAA, and SAS-70

sentrigo™

Sentrigo, Inc.
2620 Augustine Drive,
Suite 145
Santa Clara, CA 95054
USA Tel: 408.970.3300
UK Tel: +44 (0) 2076 499959
info@sentrigo.com

HE-DS-102010-01