



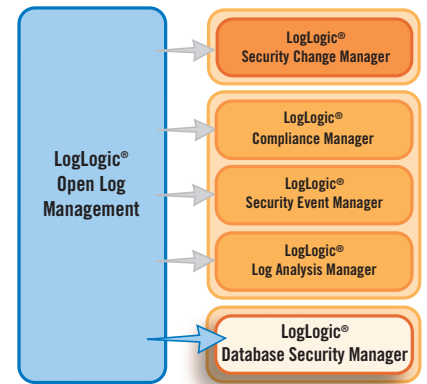
# LogLogic® Database Security Manager

## Unify Database Security Management

The need to preserve the confidentiality and integrity of data and monitor privileged user activity has driven CIOs and auditors to impose increasingly stringent controls on corporate database systems. LogLogic Database Security Manager (DSM) goes beyond native database audit functionality to provide both real-time detection and prevention solution without impacting database performance.

LogLogic DSM is an appliance based solution that is coupled with a unique host-based sensor technology to provide in-depth activity monitoring and real-time prevention of unauthorized activity. The LogLogic DSM solution helps address two critical needs of an enterprise – compliance and security. Compliance needs, focused on details such as access to Protected Health Information (PHI) or Personally Identifiable Information (PII), can not only be monitored passively, but also actively acted upon either to quarantine the user or generate critical forensic evidence for an investigation. The security needs of an organization are met by monitoring for active exploits of known database security vulnerabilities using the Virtual Patch Service.

The integration with LogLogic Open Log Management platform provides a critical element of success for an organization that is looking for a truly global picture of their enterprise activities including the database activities with the network security and operating system activities.



### Key Features and Benefits

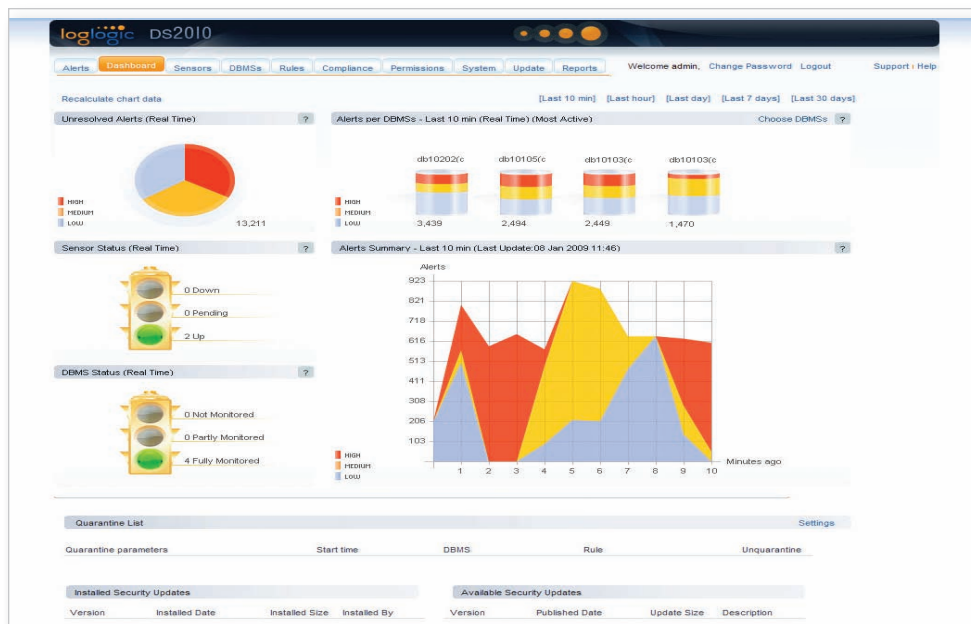
#### In-Depth Activity Monitoring

LogLogic DSM gives IT security personnel full visibility into user activity on all monitored databases. Users can create custom policies to detect security violations or use out-of-the-box rules to protect against SQL injection, buffer overflow, privilege escalation attacks, and more. By monitoring all avenues of access, including network and local connections, stored procedures and trigger executions, and encrypted or obfuscated database queries, LogLogic DSM provides in-depth audit and security monitoring of database activities to identify fraudulent or undesirable behaviors. Any PHI or PII information contained in alerts can be masked to prevent data leakage. Additionally, excessive violations can be tracked to detect fraudulent behavior.

#### Integrated Prevention Capabilities

LogLogic DSM not only issues alerts on abnormal user activities, but also stops these activities from continuing. Policies can be based on a variety of parameters, including specific database objects, SQL statements, user ID, source IP address, or applications used. Customers can prevent the loss of business data through automated connection termination and quarantine features.

(continued)



## LogLogic Database Security Manager

### System Management

- Web-based GUI (Internet Explorer, Firefox)
- Command line interface

### High Availability

- External backup capabilities
- Clustering of multiple appliances
- Hot swappable redundant power supplies
- RAID support

### Database Support

- Oracle version 8.1.7 or later, running on Sun Solaris, IBM AIX, Linux, HP/UX or Microsoft Windows
- Microsoft SQL Server 2000, Microsoft SQL Server 2005, Microsoft SQL Server 2008, running on Microsoft Windows
- Sybase ASE 12.5, running on all relevant platforms and service packs

### Operating Environment

- Hardened and optimized Linux OS

### Safety and Emissions Certification

- **Safety:** CB Report; CAN/CSA-C22.2 No 60950-1-03; ANSI/UL 60950-1-2002; EN 55022: 1998 + A1: 2000 + A2: 2003 Class A; EN 61000-3-2: 2000 + A2: 2005 & EN 61000-3-3: 1995 + A1: 2001; EN 55024: 1998 + A1: 2001 + A2: 2003
- **Emissions:** FCC Part 15 Class A, VCCI Class A, CE Class A, C-Tick, ICES, BSMI, MIC, CCC

## Key Features and Benefits (continued)

### Compliance Reporting and Forensics

Integrating database security management with LogLogic's Open Log Management platform allows customers to compare database activity to other sources of information, including network, security, server and business applications, and to integrate database sensor information into compliance reports. Protected archives of database activity records are immediately searchable, enabling enterprise-wide investigations.

### Real-Time Vulnerability Virtual Patching

LogLogic DSM's unique virtual patching technology protects the database against active exploits of known vulnerabilities without requiring affecting a database change or restart. A Virtual Patch creates a security layer around the database that helps enterprises mitigate the risks from known vulnerabilities until the time the database is patched in the environment.



## Appliance Specifications

### LogLogic DSM

Storage capacity (available)	2TB (RAID 10)
Power supply	500 watts
Chassis	2u
Ethernet	1x10/100, 4x10/100/1000
Support external disk array	Supports database servers for up to 64 CPU cores
Console configuration	9-pin serial port

## More information

Visit [www.loglogic.com](http://www.loglogic.com) or contact a LogLogic representative by e-mail: [info@loglogic.com](mailto:info@loglogic.com), or phone: 1.888.347.3883.

LogLogic is a registered trademark in the USA and/or other countries. All other brand names, product names, or trademarks belong to their respective holders. LogLogic reserves the right to alter product offerings and specifications at any time without notice, and is not responsible for typographical or graphical errors that may appear in this document.

© 2009 LogLogic, Inc. All rights reserved.

