

# Symantec™ Database Security

Proactively protects and audits against fraud and data leakage

## Overview



Traditional compliance and security measures may not be sufficient to protect against malicious database activities. Symantec™ Database Security provides real-time detection and auditing capabilities thereby reducing risks of fraud and data leakage while addressing growing compliance oversight requirements for secure information access. It detects malicious database activity from legitimate users and hackers alike and provides an audit trail for all database activity. The solution's intelligent profiling technology automatically learns "normal" database usage patterns and alerts administrators of anomalous activity.

## Key points

### *Database Compliance with Intelligent Profiling*

Self learning feature that automatically understands "normal" database activity that helps ensure compliance with policies governing access to sensitive information.

### *Monitoring and Alerting*

Proactively monitors and alerts of any database activity that falls outside the "normal" profile based on policy violations. Appliance administrators could set one of the three priorities of alerts they would like to be notified on via their preferred delivery options.

The administrators receive an alert whenever the established profiles are violated as related to either:

- Fraud Detection - potential database threats from both outsider and insider attacks
- Data Leakage - detection of credit cards, social security numbers and other custom data patterns leaving the database

### *Superior Audit Capabilities*

Real time database auditor dynamically detects anomalous SQL statements, data leakage and fraud. Helps organizations meet compliance requirements for information protection more efficiently and cost-effectively with zero performance impact.

### *Integrated Report Designer*

- Intuitive interface makes creating highly-functional reports easy.

### Appliance Requirements

- Symantec Database Security and Audit 3100 Series (SDSA 3100) is a self contained system with preloaded software components and does not have minimum system requirements. To install and setup the appliance you will need:
- A static IP address is available to assign to the appliance
- An available slot in a standard rack system to house the appliance
- Access to a browser installed on computers that has access to the same network segment as the SDSA to access the SDSA web console. The console was tested with Firefox® 1.x and Microsoft® Internet Explorer® 6.0, however the console should run well in most browsers. The console does not use advanced DHTML or require browser extensions such as ActiveX®, Flash™, or Java™.
- An available SPAN port on the network switch that handles all the incoming and outgoing traffic on the database(s) to be monitored.

Note: As an alternative to using the SPAN port on the switch, you can connect the database monitor port to a network tap. The network tap is not supplied with the appliance however these can be readily found on the market.

- To receive SNMP or SMTP alerts from the SDSA 3100 you will need the configuration information of those servers in order to configure SDSA 3100 to point to an SNMP or SMTP server within your organization.

### Supported Databases

SDSA 3100 is a database monitoring product. It can monitor the following database products:

- Oracle 8, 9, 10
- Microsoft SQL Server 2000, 2005

### Archive Tool Requirements

Accompanying the SDSA 3100 is an archive tool to periodically poll the appliance and download Incident and Event information for archival purposes. It does this by periodically connecting to the SDSA 3100, downloading data and storing that data using a separate connection to any ODBC compliance database.

The following requirements are needed for this tool.

- Standard Intel-compatible PC or laptop with at least 256MB min (512MB recommended) running one of the following operating systems:
  - Windows® 2000 with SP4 or later
  - Windows® 2003 Server with SP1 or later
  - Windows® XP with SP2 or later
- A 10/100 Base-T network connection to the same network connection as the SDSA 3100
- An ODBC connection to a database. Although any ODBC driver connection should work, the following have been tested by Symantec:
  - SQL Server, version 2000.85.1117.00
  - SQL Server, version 2000.86.1830.00
  - SQL Server, version 3.70.11.46
  - SQL Native Client, version 2005.90.1399.00
  - Oracle ODBC Driver, version 8.01.07.00

*ODBC connection to a database - continued*

- Oracle ODBC Driver, version 9.02.00.00
- Oracle ODBC Driver, version 10.01.00.02
- Microsoft ODBC for Oracle Driver, version 2.575.1117.00

**Specifications**

|                | <b>1850</b>   |
|----------------|---|
| Rack units     | 1 (1.75")   |
| Dimensions     | 76.2 cm (30") D x 48.26 cm (19") W x 4.29 cm (1.69") H                                    |
| Processor      | 2x3.0 GHz/2MB Cache Intel Xeon processor  |
| Memory         | 4 GB  |
| Storage        | 73 GB   |
| Redundancy     | Power supply, fans  |
| Administration | Centralized and Web-based, with multiple logins, administrative roles, and access control |
| Monitoring     | Support for SNMP, and email-based alerts  |
| Platform       | Linux-based operating system pre-hardened against common vulnerabilities and attacks      |

**More information**

*Visit our web site*

<http://enterprise.symantec.com>

*To speak with a Product Specialist in the US*

Call toll-free (800) 745-6054

*To speak with a Product Specialist outside the US*

Symantec has operations in 40 countries. For specific country offices and contact numbers, visit our web site.

*About Symantec*

Symantec is the world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information.

Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. More information is available at [www.symantec.com](http://www.symantec.com).

*Symantec World Headquarters*

20330 Stevens Creek Blvd.

Cupertino, CA 95014 USA

(408) 517-8000

(800) 721-3934

[www.symantec.com](http://www.symantec.com)

