



## SecureSphere® Database Activity Monitoring

Gain Visibility into Database Activity

*Audit and secure your database data through real-time monitoring and event analysis. SecureSphere helps businesses:*

- » *Capture complete database activity details*
- » *Leverage flexible views and audit analytics to make audit data accessible*
- » *Generate real-time alerts on database attacks and fraudulent activity*
- » *Build a data security and compliance lifecycle*
- » *Automate and centralize database auditing and reporting*

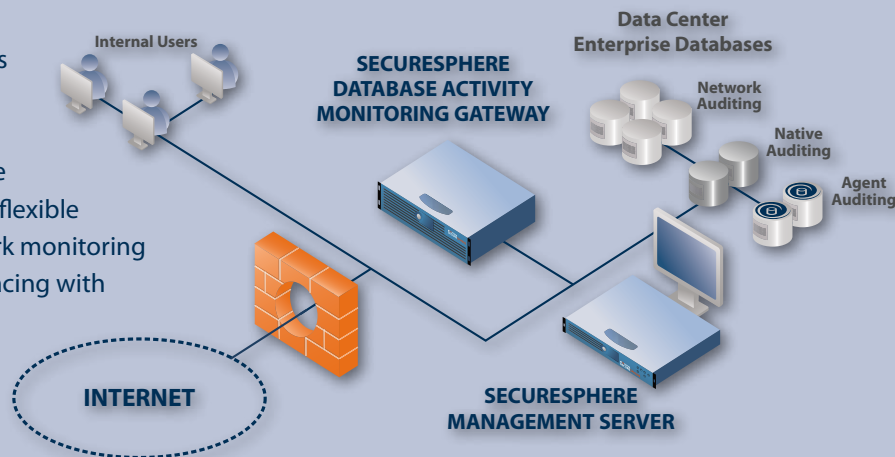
**Database Activity Monitoring**



**Only the market leading  
SecureSphere Database  
Activity Monitoring delivers  
complete visibility into  
database activity.**

## Unparalleled Database Visibility

SecureSphere Database Activity Monitoring provides visibility and protection for all major database platforms including Oracle, MS-SQL, IBM DB2, Sybase, Informix, MySQL and Teradata. SecureSphere supports all collection methods and offers the most flexible deployment options. Deployed as non-inline network monitoring appliances, coupled with light weight agents, interfacing with native database auditing tools, or working a hybrid combination, SecureSphere provides visibility into all activity types, including local privileged activity. It establishes a detailed and independent audit trail of database activity in a tamper-proof repository. A centralized management server enables unified management of distributed gateways and agents.



The SecureSphere Database Activity Monitoring (DAM) solution is designed to provide the industry's best automated auditing and security for critical database platforms. It helps organizations gain visibility into their database activity and understand their risk posture through discovery and assessments, continuous auditing, and effective measurements.

### Addressing PCI-DSS Compliance with SecureSphere DAM

PCI-DSS requirements emphasize the importance of real-time monitoring of access to cardholder data. SecureSphere enables merchants and service providers to address the most challenging PCI requirements quickly, painlessly, and cost effectively. SecureSphere provides compensating controls for database encryption (PCI-DSS 3). It also enables critical monitoring and tracking of all access to cardholder data (PCI-DSS 10).

Additional PCI-DSS requirements are addressed through:

- Built-in assessments to confirm vendor supplied accounts and passwords are not in use
- Intelligent alerts on unauthorized access to cardholder data
- Built-in and custom reports to measure effectiveness of controls

Overall, 7 out of the 12 PCI-DSS requirements are addressed by SecureSphere Database Activity Monitoring. Additional PCI requirements are addressed through SecureSphere Database Firewall and Database Security Suite.

## Discovery and Vulnerability Management

### Database Discovery and Classification

SecureSphere ensures that organizations can prioritize and protect all sensitive data. Network based discovery of database servers throughout the network ensures awareness. Classifying databases based on the data types they contain helps organizations map and prioritize the discovered servers and fundamentally understand which servers are within the scope of a regulatory compliance project.

### Comprehensive Vulnerability Assessment

SecureSphere includes a full set of platform assessment tests, RDBMS vulnerabilities and best practices to help organizations remediate and control the configuration of their database environments and implement an overall vulnerability management strategy.

The assessments are kept up-to-date with the latest research from the Imperva Application Defense Center (ADC) research team.

### Intelligent Behavioral Assessments

Behavioral assessment delivers unique visibility into how users and applications are actually accessing and manipulating database data. SecureSphere builds a comprehensive usage profile for analysis and reporting that shows activity details like time/date, source/destination, user, client application, and can be used to spot abnormal activity.

## Automated Auditing and Security

SecureSphere includes a complete set of predefined audit and security policies which can be quickly implemented for

monitoring any database environment. These policies are based on 'Black-list' and 'White-list' security modules which are continuously updated through Imperva's patent pending Dynamic Profiling Technology and updated research conducted by the Imperva ADC.

The Dynamic Profiling technology automatically detects and incorporates valid changes over time, and relieves administrators from the need to manually create and update tedious white lists that contain hundreds and thousands of objects, users and SQL queries.

## Continuous Audits and Analysis of all Database Traffic

Granular auditing and continuous monitoring of all database operations in real-time provides organizations with a detailed audit trail that shows the 'Who, What, When, Where and How' of each transaction. SecureSphere captures all database activity including DML, DDL and DCL activity, read-only activity (SELECTs), changes made to stored procedures, triggers and database objects, as well as SQL errors and database login activity. SecureSphere also monitors (and optionally audits) the database response to ensure there is no leakage of sensitive data.

### Managing Security and Change

SecureSphere monitors database activity in real time and looks for various database attacks at the OS, protocol level, and SQL level. Granular row-level change auditing enables accurate alerts on fraudulent activity, database changes, and attacks – sending real-time alerts, assigning followed tasks, and ensuring change control.



## Database Auditing Aspects of SOX Compliance

SOX sections 302 and 404 require that appropriate steps and controls are implemented to ensure consistent production of reliable financial information (Section 302) and the reliability of internal control (Section 404).

SecureSphere enables organizations to keep an independent audit trail which provides detailed information on the 'Who, What, When, Where and How' on activity related to financial data, supporting the enforcement of access controls and ensuring the integrity of financial data.

Built-in audit analytics views and reports help organizations address SOX specific requirements like identification of dormant accounts, monitoring of failed logins and implementation of change controls.

### Independent Monitoring and Auditing

As an independent monitoring solution, SecureSphere does not require enablement of native auditing tools, nor does it rely on the DBA for implementation and maintenance. SecureSphere leverages gateway appliances to monitor network traffic, and light-weight SecureSphere agents to capture local activity and eliminate blind spots. This non-intrusive hybrid architecture ensures audit independence and separation of duties.

### Tamper-Proof Audit Trail

SecureSphere captures the detailed audit trail in an external, secured and hardened repository which can be accessed through read-only views. The repository enforces a role based access mechanism (RBAC) for administrative and security usage. To ensure the integrity of the audit trail it can also be encrypted.

### Streamline Compliance Efforts

#### Interactive Audit Analytics

Complete visibility into audited activities is provided through interactive audit analytics, which enables non-technical database auditors to analyze, correlate,

and view database activity from virtually any angle with just a few mouse clicks, enabling easy identification of trends and patterns that may conceal security risks or compliance problems.

### Best-in-Class Reporting

SecureSphere provides easy reporting on audited events with predefined graphical reports that help measure risk and address regulatory requirements. Specific reports are designed for demonstrating compliance with SOX, PCI, and other data privacy laws. Scheduling automated reports, sending the results in PDF or HTML formats, and integration with SIEM, ticketing systems and other 3rd party solutions streamlines business processes.

### Risk Management for Databases

SecureSphere significantly reduces the efforts required to effectively and efficiently manage risk to data. Enterprise risk management dashboards and drill-down views help organizations establish mitigating controls to prevent data loss and information leaks, reducing the risk of unauthorized access and fraudulent activity.

### Flexible Deployments, Low TCO

#### Flexible Deployment Modes: Network, Agent, Native Audit, or Hybrid

SecureSphere offers the most flexible deployment options, offering non-intrusive network monitoring, lightweight agent monitoring, native audit collection, or a hybrid mix. This enables organizations to deploy whatever mix fits their unique topology and business needs.

### Performance and Scalability

Unmatched by any other DAM solution, SecureSphere provides fast processing and complete audit capabilities that can easily scale to support any environment – from SMBs to large Enterprise.

### Centralized Management

SecureSphere offers centralized management for SecureSphere gateways. This enables better efficiency and effectiveness in large-scale SecureSphere deployments. And support for hierarchical policy management and administrations supports even the largest organizations.

### Monitoring and Validating Privileged Database Activity

Privileged users and DBAs are responsible for the administration and maintenance of databases and require elevated privileges and access to system resources. Complete visibility into privileged activity and real-time alerts ensure that only authorized applications and users are accessing sensitive data, or performing changes to database schemas and values. SecureSphere light-weight agents eliminate blind spots and ensure full capturing of all network and local privileged operations including Data Definition Language (DDL) commands and Data Control Language (DCL) commands as well as Data Manipulation Language (DML) commands and SELECTs. Monitoring privileged users' activity is critical for fully protecting databases against internal fraud and abuse as well as external attacks.

## SecureSphere Features and Appliance Specifications

### Coverage

Oracle, MS-SQL, Sybase, DB2, Informix, MySQL, Teradata

### Deployment Modes

Flexible Hybrid deployments combining – Network Monitoring Gateways: Inline or in sniffing mode

SecureSphere Agents: light-weight agents monitor local privileged activity

Remote agentless collection: for 3rd party audit logs

### Discovery & Classification

Database Servers, Financial Information, Credit Card Numbers, System and Application Credentials, Personal Identification Information, Custom Data Types

### Vulnerability Assessment

Operating system and RDBMS vulnerabilities Configuration and Security Best Practices

### User Activity Details

Network and Local user activity

Database User, source OS user, User group

### SQL Operations

Read-Only (SELECTs), Data changes (DML), changes to Objects and Schemas (DDL), User creation, grants and revokes (DCL)

### Query Details

Query Text, query group, response text, response size, response time, response codes, response code strings

### Complex Queries

Prepared statements, nested and dynamic queries, views, triggers, stored procedures and the operations they execute

### Event Details

Date, Time, Source OS, Source Application, Source hostname, user location, database location

### Platform Security

Platform intrusion prevention

Known and zero-day worm security

### Network Security

Stateful firewall

DoS prevention

### Fraud Prevention

Unauthorized sensitive data access

Unexpected source IP or time of day

Abnormal user activity

### Data Leak Prevention

Credit card number

PII (personally identifiable information)

Pattern matching

### Content Updates

Signatures and content updates based on primary ADC research delivered through ADC Updates

### Tamper-Proof Audit Trail

Optional encryption of audit data

Role based access controls to real-time views of audit data (read-only)

### Centralized Management

MX Server for centralized management

Web User Interface (HTTP/HTTPS)

Command Line Interface (SSH/Console)

Real-time dashboard

### Integrated Reporting

Predefined graphical reports including:

- » Compliance (SOX, PCI, HIPAA and more)
- » Business applications (SAP, Oracle EBS, PeopleSoft)

Custom User defined Reports

### Workflow and 3rd Party Integration

SNMP, Syslog, Email

SecureSphere task workflow

SIEM and Incident management ticketing integration

### High Availability

IMPVHA (Active/Active, Active/Passive)

Fail open interfaces (bridge mode only)

VRRP

STP and RSTP

Specification	SecureSphere G4 FTL	SecureSphere G8 FTL	SecureSphere G16 FTL
Throughput	500 Mbps	1,000 Mbps	2,000 Mbps
Transactions/Sec	50,000	100,000	200,000
Latency	Sub-millisecond	Sub-millisecond	Sub-millisecond
Interfaces	6 x 10/100/1000 Mbps (max 4 Fiber interfaces)	6 x 10/100/1000 Mbps (max 4 Fiber interfaces; optional 10 Gbps interfaces)	6 x 10/100/1000 Mbps (max 4 Fiber interfaces; optional 10 Gbps interfaces)
Interface Types	Copper/Fiber SX/Fiber LX	Copper/Fiber SX/Fiber LX	Copper/Fiber SX/Fiber LX
Max Network Segments	(2)Bridge; (5)Router, Non-inline	(2)Bridge; (5)Router, Non-inline	(2)Bridge; (5)Router, Non-inline
Form Factor	2U 19-inch rack	2U 19-inch rack	2U 19-inch rack
Hard Drive	(2) Hot-Swap 250GB SATA	(2) Hot-Swap 250GB SATA	(2) Hot-Swap 250GB SATA
Power Supply	(2) Hot-Swap 750W total	(2) Hot-Swap 750W total	(2) Hot-Swap 750W total
AC Power	100-240V, 50-60 Hz	100-240V, 50-60 Hz	100-240V, 50-60 Hz



### Imperva

North America Headquarters  
3400 Bridge Parkway  
Suite 101  
Redwood Shores, CA 94065  
Tel: +1-650-345-9000  
Fax: +1-650-345-9004

International Headquarters  
125 Menachem Begin Street  
Tel-Aviv 67010  
Israel  
Tel: +972-3-6840100  
Fax: +972-3-6840200

Toll Free (U.S. only): +1-866-926-4678  
www.imperva.com

© Copyright 2009, Imperva

All rights reserved. Imperva and SecureSphere are registered trademarks of Imperva.

All other brand or product names are trademarks or registered trademarks of their respective holders. #DS-DAM\_0409rev1