



SecureSphere® Database Monitoring Gateway

Automated, Scalable Activity Monitoring,
Audit and Reporting for Business
Applications and Databases

Regulatory compliance and best practice standards are driving the need to monitor and audit the information residing within sensitive business applications and databases.

The SecureSphere Database Monitoring Gateway is an automated, scalable database activity monitoring, auditing and reporting solution for business applications and databases.



SecureSphere Database Monitoring Gateways

SecureSphere Database Monitoring Gateways are a family of automated database audit appliances for Oracle, MS-SQL, IBM DB2 (including mainframe), Sybase, and Informix environments. Deployed as non-inline network monitors, SecureSphere gateways establish a detailed, independent record of database application activity of any kind with specific emphasis on packaged applications like Oracle E-Business Suite, SAP and PeopleSoft. A lightweight host agent is also available to monitor the local (e.g. console, telnet, ssh, IPC, and shared memory) activity of database administrators. Although SecureSphere may be deployed as a standalone appliance, a centralized management server enables unified management of distributed gateways and agents.

SecureSphere Highlights

- » Universal User Tracking links database activity to users connected through application servers over pooled connections.
- » Dynamic Profiling automatically creates verified user activity profiles and identifies material variances.
- » Distributed Audit Architecture enables detailed data collection while preserving scalability.
- » Unified auditing of mixed MS-SQL, Oracle, DB2, Sybase, and Informix environments automate integration of multi-vendor logs.
- » Network appliance and local host agent deployment ensures that all database activity is monitored.
- » Transparent deployment simplifies implementation with no impact on database performance or availability.

Audit and Activity Monitoring

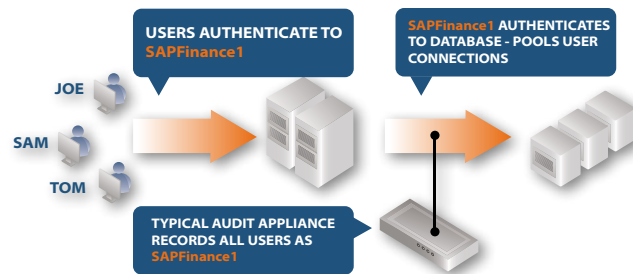
User Accountability

A primary objective of any database audit is to validate that user accountability has been established. A SOX compliant audit, for example, must log each change to financial reporting data along with a unique identifier (first/last, userid, etc.). Many database audit solutions do not meet this requirement beyond the most basic user authentication scenarios.

SecureSphere's Universal User Tracking technology makes individual users accountable under any authentication scenario by combining multiple user identification methods. Database account names and source IPs identify DBAs with direct query access rights. OS hostnames and usernames identify users of shared root privilege accounts. Database transactions are correlated with Web application logins and sessions to track users who authenticate to a Web application and are then aggregated under a single account name (connection pooling). Finally, SecureSphere applies custom algorithms to identify users who authenticate via multi-tier business applications such as SAP, and Oracle EBS.

Verified User Profiles and Material Variances

Auditors require organizations to track material variances from normal authorized access behavior. To meet the need to identify material variances, SecureSphere's Dynamic Profiling technology applies sophisticated learning algorithms to automatically create and maintain verified baseline profiles of each user's normal behavior. Compliance staff may then compare the profiles with user job functions, regulatory requirements, or best practices. Profiles may be optionally modified,



approved, and converted into authorized policies which SecureSphere applies to automatically identify material variances over time.

Row Level Change Auditing

Streamlining fraud prevention, forensics, and SOX compliance, SecureSphere automatically identifies and alerts organizations to suspicious changes to the values of specific records or subsets of table rows. Unlike invasive "trigger-based" approaches, SecureSphere's non-intrusive approach is completely transparent to the target database.

Complete Assessment

SecureSphere uniquely provides three distinct assessment capabilities: server & sensitive data discovery, configuration assessment and behavior assessment. Together, these capabilities provide the targeted information needed to define the baseline of configuration and usage of data, identify risk, prioritize any required corrective actions or mitigating controls, and document compliance.

Server & Sensitive Data Discovery simplifies the discovery of sensitive data. SecureSphere scans a network IP range first for the existence of all database and web/application servers. Then, it can scan within each database for sensitive data such as credit card numbers, social security numbers, national ID numbers, etc. Even encrypted data can be identified and monitored.

Configuration Assessment queries the database for configuration information, including compliance with over 500 security tests and other information on important characteristics of the database. Testing covers five key areas including user privileges, software configuration, known software flaws, external objects, and compliance to best practices.

Behavior Assessment identifies vulnerabilities that can only be identified by monitoring activity over time. For example, login events are analyzed over time to detect shared usage accounts by multiple users – a clear security violation emphasized by most IT control frameworks.

Independence and Separation of Duties

To ensure integrity, the audit should be independent of the database server and

separate audit duties from database administration. For example, an audit that relies on built-in audit capabilities can be easily compromised by a rogue DBA who disables audit functions.

SecureSphere enables separation of duties between audit and database functions. It can be deployed without database privileges, without change to database configuration, and it can be operated by functional, audit or security staff without skilled DBA expertise.

Operations

Detail and Scalability

SecureSphere's Distributed Audit Architecture enables both detailed logging and enterprise-level scalability. The architecture distributes audit collection, data storage and analytical processing across multiple high performance DMG appliances. The SecureSphere management server presents high-level audit views from a unified console. When compliance managers need to drill down from high-level views to detailed logs, the management server automatically retrieves the required information from the distributed gateways.

To deal with very large data sets and long term data retention requirements, audit information may be periodically archived to external devices. To preserve data integrity and reduce storage requirements, archived data can be encrypted, signed and compressed. Access to archived data is controlled from the SecureSphere audit viewing interface.

Flexible Audit Policy Definition

SecureSphere's audit policy wizard allows specification of audit criteria in a matter of minutes. A rule may specify comprehensive tracking of all sensitive data transactions, or selective tracking based on a combination of attributes (see SecureSphere Audit Information Table). In addition, multiple rules may operate in parallel to track data access from different perspectives. For example, one rule may focus on all access to a specific table, while another focuses only on table changes. ADC Insights provide extremely targeted rules, assessments, reports and more for specific applications and mandates.

Business Relevant Reporting

A generic audit solution that simply logs mountains of database transactions does not answer the specific audit questions relevant to different industries, applications, regulations, and best practice frameworks. Data must be analyzed and presented to auditors in a format that has relevance to specifics of each business.

SecureSphere's graphical reporting framework integrates the analytical tools

needed to document compliance with relevance to specific business environments.

The market's most complete set of compliance reports accelerates the audit against a range of regulations/best practice frameworks including SOX, HIPAA and PCI.

These reports focus not only on specific regulatory criteria, but on criteria relevant to business applications such as SAP and Oracle EBS. No other database audit solution delivers the ability to focus on the audit questions relevant to specific regulatory issues and business applications.

SecureSphere reporting also supports scheduling, customization and data export to external reporting tools.

Complete Local Monitoring

The lightweight SecureSphere DBA Monitor Agent tracks all local/console database activity including telnet, ssh, and IPC/shared memory. All agent communications can be encrypted and audit data is buffered locally to prevent loss in the event of network downtime. Together, SecureSphere agents and appliances ensure complete monitoring of all activity.

Timely Response

SecureSphere's real time alerts enable immediate response to variances if desired. Granular alert policies can be flexibly configured for a range of variances including: user profile violations, audit evasion attempts, privileged SQL operations, and network access control policy violations. Even specific correlations of these variances can trigger alerts.

ADC Insights – Business Relevant Knowledge

In addition to SecureSphere Database Gateways, Imperva offers unique Insights products – predefined audit, compliance and security content and report templates that keep you up-to-date with the latest in-depth knowledge about specific applications like SAP and Oracle EBS.

Deployment

Transparent Network Deployment

SecureSphere appliances deploy as transparent network monitors without change to the network, applications, or databases. They have no impact on database performance and introduce no single point of failure.

Centralized Management

SecureSphere can be deployed as a standalone appliance or distributed across large data centers. For large environments, the SecureSphere Management Server centralizes configuration, monitoring, and reporting. Management is further streamlined through hierarchical groupings (customers, business units, locations, etc.), role-based administrative permissions, and unique task-oriented workflow. SecureSphere administrators can be authenticated via internal or external-LDAP authentication databases.



SecureSphere monitors all access to and all activity occurring in databases. Out-of-the-box reports help quickly identify unauthorized activity and adherence to compliance regulations.

SecureSphere Audit Information – Deep Activity Monitoring

User	Database username, Web app. username, source OS username, user group
Data	Database, schema, table, column, bind variables
Operations	All SQL operations – DML, DDL, DCL
Query	Query text, query group, response text, response size, response time, response codes, response code strings
Programs	Prepared statements, nested and dynamic queries, stored procedures and the operations they execute
Context	Date, time, source OS, source application, source URL, source hostname, user location, database location
Variances/Alerts	Profile, best practice configuration, best practice behavior, data leakage, audit evasion attempts (IPS/protocol violation), privileged SQL operations

SecureSphere Appliance Specifications

Specification	SecureSphere G4	SecureSphere G8	SecureSphere G16
Throughput	500 Mbps	1000 Mbps	2000 Mbps
SQL 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)	6 x 10/100/1000 Mbps (max 4 fiber interfaces)
Interface Types	Copper/Fiber SX/Fiber LX	Copper/Fiber SX/Fiber LX	Copper/Fiber SX/Fiber LX
Max Segments	5	5	5
Form Factor	2U	2U	2U
Hard Drive	(2) Hot-Swap 250GB SATA	(2) Hot-Swap 250GB SATA	(2) Hot-Swap 250GB SATA
External Drive	CD-ROM	CD-ROM	CD-ROM
Enclosure	19 inch rack	19 inch rack	19 inch rack
Weight	65 lbs	65 lbs	65 lbs
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
Dimensions	16.93" x 27.75" x 3.44"	16.93" x 27.75" x 3.44"	16.93" x 27.75" x 3.44"
Operating Environment	10°C (50°F) to 35°C (95°F)	10°C (50°F) to 35°C (95°F)	10°C (50°F) to 35°C (95°F)
Non-Operating Environment	-40°C (-40°F) to 70°C (158°F) relative humidity 90%, non-condensing at 35°C (95°F)	-40°C (-40°F) to 70°C (158°F) relative humidity 90%, non-condensing at 35°C (95°F)	-40°C (-40°F) to 70°C (158°F) relative humidity 90%, non-condensing at 35°C (95°F)
EMC Certifications	FCC, CISPR 22, CE, VCCI	FCC, CISPR 22, CE, VCCI	FCC, CISPR 22, CE, VCCI

Specification	MX Management Server
Form Factor	1U; Fault Tolerant Model: 2U
Interfaces	2 x 10/100/1000 Mbps Copper
Hard Drive	250GB SATA; Fault Tolerant Model: (2) hot-swappable 250GB SATA
External Drive	CD-ROM
Enclosure	19 inch rack
Weight	25 lbs; FTL Model: 65 lbs
Power Supply	350W; Fault Tolerant Model: (2) hot-swappable 750W total
AC Power	100-240V, 50-60 Hz
Dimensions	16.93" x 25.51" x 1.67"; FTL Model: 16.93" x 27.75" x 3.44"
Operating Environment	10°C (50°F) to 35°C (95°F)
Non-Operating Environment	-40°C (-40°F) to 70°C (158°F) relative humidity 90%, non-condensing at 35°C (95°F)
EMC Certifications	FCC, CISPR 22, CE, VCCI

Imperva

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

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

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

