



SecureSphere® Database Monitoring Gateway

Automated, Scalable Activity Auditing
and Reporting for Databases

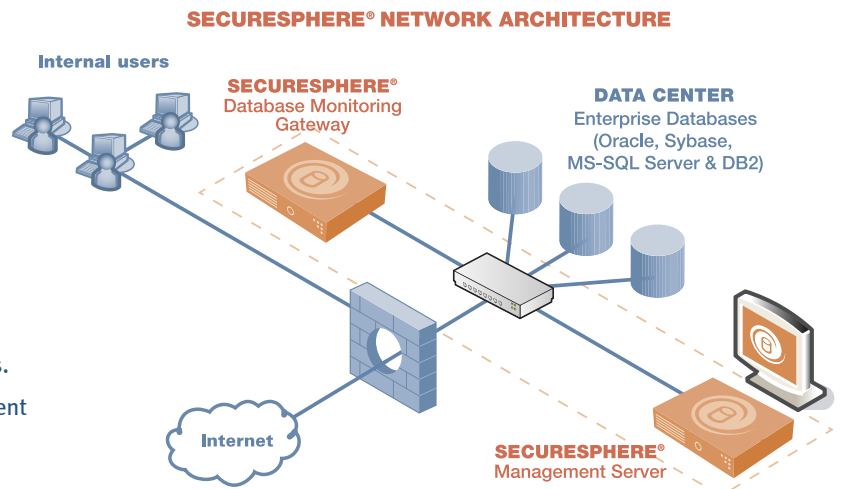
Government regulations and industry standards are driving organizations to expand audit processes to the sensitive information stored within corporate databases. Auditors and information technology (IT) professionals must work together to prove that data usage in Oracle E-Business Suite, SAP, PeopleSoft and other package or custom applications meets the control requirements of SOX and other regulations. Database Administrator (DBA) activity must also be monitored and compared against organizational policies and controls.

Unfortunately, auditing mission critical database systems is no simple task. These systems serve a wide range of users (each with their own distinct privileges), must support high transaction rates and meet demanding service level requirements. The audit capabilities built into commercial database software fail to meet the fundamental audit requirement for independence, plus they degrade database performance and dramatically increase ongoing administrative costs. Third party auditing products attempt to address these issues but fail to track all of the information demanded by auditors.



SecureSphere Database Monitoring Gateways

SecureSphere Database Monitoring Gateways are a family of automated database audit appliances for MS-SQL, Oracle, DB2 and Sybase environments. Deployed as non-inline network monitors, SecureSphere gateways establish a detailed, independent record of database activity for packaged applications like Oracle E-Business Suite, SAP and PeopleSoft as well as custom Web applications. A dedicated host agent is also available to monitor the local (e.g. console, telnet, ssh) activity of database administrators. A centralized management server enables unified management of multiple distributed gateways and agents.



Auditing

User Accountability

One of the primary objectives of any database audit process is validation that user accountability has been appropriately established for every database transaction. For example, a SOX compliant audit mechanism must log each change to financial reporting data along with the specific name of the end user of the system (first/last, userid or similar unique identifying information). Unfortunately, application users login to the application and not the database. Instead all database access is done over a single database connection (connection pooling). This means the individual usernames are not available to the database and therefore can not be recorded by existing database audit solutions.

SecureSphere's Universal User Tracking technology makes individual users accountable – even when they access data through packages (Oracle, SAP, PeopleSoft, etc) or custom Web applications. To identify usernames, a dedicated SecureSphere interface monitors application user activity and correlates it with database transactions. In the context of the previous SOX example, Universal User Tracking enables SecureSphere to link changes to financial records with the specific username of the person making the change via the package or custom application.

Verified User Profiles and Material Variances

Auditors require organizations to track material variances from authorized data access privileges. This is often an overwhelming task given that a baseline understanding of each user's appropriate usage requirements is not readily available.

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 representing each user's normal behavior. Compliance staff may then compare the profiles to regulatory or best practice requirements. Profiles may be modified (optionally), approved and converted into policies which SecureSphere applies to automatically identify material variances over time.

Best Practices Security Assessment

In addition to evaluation of access privileges and variances, auditors must assess the configuration of the underlying database server. What software patch levels are installed? Is the database configured according to best practices? Satisfactory answers to these and other questions are critical to the compliance process.

SecureSphere uniquely provides both active and passive database assessment. Active

assessment polls the database for hundreds of configuration vulnerabilities including database software versions, OS versions, weak passwords, excessive user privileges and more.

Passive assessment reveals weaknesses that only become apparent through monitoring of actual activity. Examples include shared login credentials and non-DBA access to sensitive database elements such as default stored procedures, default user accounts, system objects and the like.

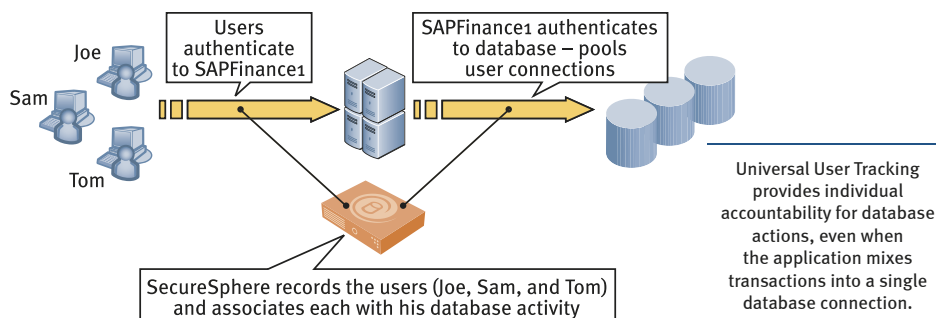
Imperva's Application Defense Center, an international security research organization, provides regular updates to the assessments to ensure that the most current best practices are in use.

Independence and Separation of Duties

An often overlooked aspect of database audit is the integrity of the process itself. 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 database audit capabilities can be easily compromised by a rogue database administrator (DBA) who disables audit functions.

As an independent appliance, SecureSphere enables separation of duties between audit and database administration functions. It can be deployed without database privileges and without any change to database configuration. Role-based administration ensures separation of duties between the database administrators who manage the database and the auditors or security staff that administer SecureSphere.

Finally, to prevent a user from exploiting server software vulnerabilities to disable auditing or avoid authentication (and thus, accountability), SecureSphere's database



Intrusion Prevention System (IPS) with the industry's only SQL protocol validation capabilities logs any attempts to evade the auditing mechanism. With SecureSphere, compliance staff can be confident in the integrity of the audit process and the completeness of the audit log.

Detail and Scalability

Compliance staff often face a difficult trade off in designing audit processes – detailed logging versus enterprise-level scalability. To provide auditors with the information they demand, the audit system must record database activity down to the level of the actual query and response. On the other hand, such query-level logging consumes vast storage and CPU resources making audit of enterprise class applications like Oracle E-Business Suite and SAP particularly challenging.

To deal with scalability problems, many audit systems only record the actual query and response for low volume environments. In medium or high volume environments, these products record only basic information such as user names, database commands (i.e. SELECT), and tables (i.e. CUSTOMER_RECORDS). Even worse, some systems do not record independent events, but record only an aggregation of events (e.g. Joe accessed CUSTOMER_RECORDS 10 times.) Unfortunately, such a system is blind to critical detail. Which customer records were viewed? Was financial data changed? Were credit cards compromised?

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 auditors to specify custom audit criteria in a matter of minutes. A rule may specify comprehensive tracking of all database activity regarding sensitive data, 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.

Reporting

An audit solution that simply logs mountains of database transactions does not answer the specific data usage questions posed by auditors. Audit information must be aggregated, filtered, sorted and presented to auditors in a clear format that answers specific questions.

SecureSphere's integrated graphical reporting capabilities provide auditors with the analysis tools they need to quickly evaluate specific data usage questions. A wide range of preconfigured reports relevant to virtually any environment are included. In addition, compliance reporting packages are available to address the specific requirements of Sarbanes-Oxley (SOX), the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry (PCI) standard. SecureSphere reporting information is also accessible to external reporting tools or any ODBC-compliant database access tool.

Timely Response

Most audit systems are limited to postmortem analysis of database events. SecureSphere's real time alerts enable immediate incident evaluation and remediation if necessary.

Deployment

Transparent Deployment

SecureSphere can be deployed with no impact on the IT infrastructure. As a network monitor, SecureSphere introduces

SecureSphere Highlights

- Universal User Tracking associates database activity with end users of connected SAP, Oracle E-Business Suite, or other Web-based applications.
- Dynamic Profiling automatically creates verified user activity baselines and identifies material variances.
- Distributed Audit Architecture enables detailed data collection while preserving scalability for large data centers.
- Unified auditing for mixed MS-SQL, Oracle, DB2, and Sybase environments enables consistent audit policy and eases integration of multi-vendor logs.
- Network appliance and local host agent deployment ensures that all database activity is monitored.
- Transparent deployment enables quick implementation with no impact on database performance or availability.

no single points of failure. It requires no changes to the network, applications, or the database and it has no impact on database performance. Transparent Deployment enables quick audit implementation with zero risk to the availability and performance of SAP, Oracle applications, or any other mission critical systems being audited.

Monitoring Local Database Access

For cases in which database operations are performed locally on the server, SecureSphere monitors activity via the SecureSphere DBA Monitor Security Agent. The SecureSphere DBA Monitor provides a low-footprint capability to capture console-based access to the database. This activity is forwarded to the SecureSphere gateway for processing and analysis, limiting the impact of the agent on the performance of the database server.

Centralized Management

SecureSphere gateways can be deployed as standalone audit appliances with integrated single-device management. Alternatively, the MX Management Server provides centralized management for multi-gateway deployments. The MX Management Server unifies policy management, logging, reporting and alerting across multiple gateways. Redundant management servers may be deployed to ensure continuous access to audit processes.

SecureSphere Audit Information

User	Database username, Web application username, source OS username, user group
Data	Database, schema, table(s) and column(s)
Operations	All SQL operations – DML, DDL, DCL, stored procedures
Query	Query text, query group, response content, response size, response time, response codes, response code strings
Context	Date, time, source OS, source application, source URL, source hostname, user location, database location
Variances/Alerts	Usage Exceptions and Variances, Best Practice Configuration, Best Practice Behavior, Audit Evasion Attempts (IPS/Protocol Violation), Privileged SQL Operations

SecureSphere Appliance Specifications

Specification	G4	G8	G16
Throughput	500 Mbps	1000 Mbps	2000 Mbps
SQL Transactions / Sec	50,000	97,000	140,000
Latency	Sub-millisecond	Sub-millisecond	Sub-millisecond
Form Factor	1U	1U	4U
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
Hard Drive	250GB SATA; Fault Tolerant Model: hot-swappable 250GB SATA	250GB SATA; Fault Tolerant Model: hot-swappable 250GB SATA	Hot-Swappable 300GB SCSI
External Drive	CD-ROM	CD-ROM	DVD-ROM
Enclosure	19 inch rack	19 inch rack	19 inch rack
Weight	40 lbs (18Kg)	40 lbs (18Kg)	90lbs (41Kg)
Power Supply	500W; Fault Tolerant Model: Dual, hot-swappable 520W	500W; Fault Tolerant Model: Dual, hot-swappable 520W	Dual, hot-swappable 1470W
AC Power Supply	100-240V, 50-60 Hz	100-240V, 50-60 Hz	220-240V, 50-60 Hz
Dimensions	W 16.93" (430mm) D 26.46" (672mm) H 1.7" (43mm)	W 16.93" (430mm) D 26.46" (672mm) H 1.7" (43mm)	W 17.6" (447mm) D 27.8" (706mm) H 6.8" (173mm)
Operating Environment	5°C (41°F) to 35°C (95°F)	5°C (41°F) to 35°C (95°F)	5°C (41°F) to 35°C (95°F)
Non-Operating Environment	-40°C (-40°F) to 70°C (158°F) relative humidity 95%, non-condensing at 35°C (95°F)	-40°C (-40°F) to 70°C (158°F) relative humidity 95%, non-condensing at 35°C (95°F)	-40°C (-40°F) to 70°C (158°F) relative humidity 95%, non-condensing at 35°C (95°F)
Electromagnetic Capability	FCC Part 15, ICES-003, CE, VCCI	FCC Part 15, ICES-003, CE, VCCI	FCC Part 15, ICES-003, CE, VCCI

Specification	MX Management Server
Form Factor	1U
Interfaces	2 x 10/100/1000 Mbps Copper
Hard Drive	250GB SATA; Fault Tolerant Model: hot-swappable 250GB SATA
External Drive	CD-ROM
Enclosure	19 inch rack
Weight	40 lbs (18Kg)
Power Supply	500W; Fault Tolerant Model: Dual, hot-swappable 520W
AC Power Supply	100-240V, 50-60 Hz
Dimensions	W 16.93" (430mm), D 26.46" (672mm), H 1.7" (43mm)
Operating Environment	5°C (41°F) to 35°C (95°F)
Non-Operating Environment	-40°C (-40°F) to 70°C (158°F) relative humidity 95%, non-condensing at 35°C (95°F)
Electromagnetic Capability	FCC Part 15, ICES-003, CE, VCCI

Imperva Inc.
U.S. Headquarters
950 Tower Lane
Suite 1550
Foster City, CA 94404
Tel: (650) 345-9000
Fax: (650) 345-9004

International Headquarters
12 Hachilazon Street
Ramat-Gan 52522
Israel
Tel: +972-3-6120133
Fax: +972-3-7511133



eWEEK Excellence Award
Network Data-Stream Protection
June 19, 2006
SecureSphere 4.2



ORACLE PARTNER



Toll Free (U.S. only): 866-592-1289
www.imperva.com