



SecureSphere® Database Security Gateway

Usage Assessment, Audit and Protection
for Business Applications and Databases

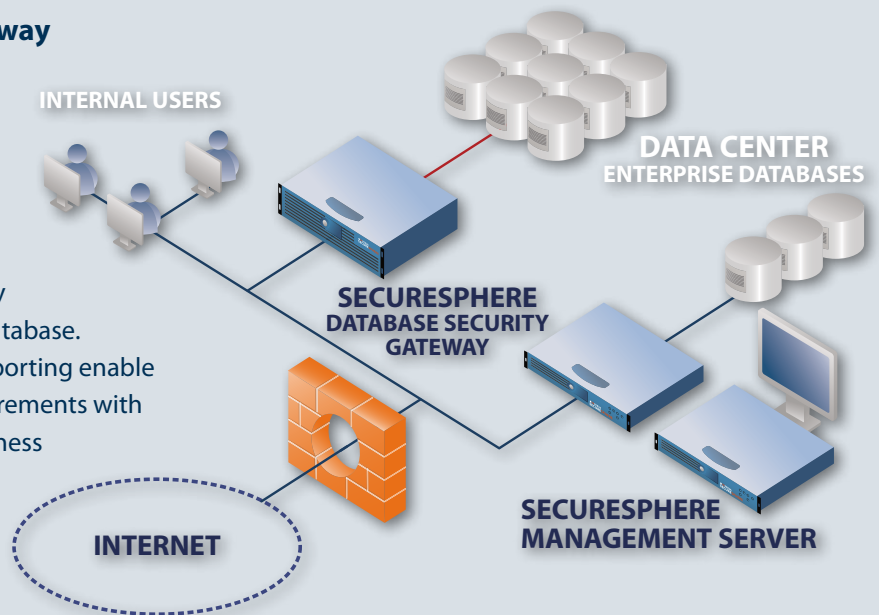
Data theft, misuse, and leakage have combined with increasingly stringent compliance requirements to drive the need to apply more robust security assessment, audit and protection processes to sensitive business applications and databases.

The SecureSphere Database Security Gateway is a complete usage assessment, audit, and protection solution for business applications and databases.



The SecureSphere Database Security Gateway

The SecureSphere® Database Security Gateway provides automated activity monitoring, audit and protection for Oracle, MS-SQL Server, IBM DB2 (including mainframe), Sybase, and Informix databases. Dynamic Profiling technology automatically creates database usage profiles and security policies that are granular down to the query level for every user and application accessing the database. Detailed database activity monitoring, audit and reporting enable streamlined compliance with regulatory audit requirements with zero impact on database performance. Unique business activity analysis and correlation technologies provide real-time governance and protection by separating out real risks and attacks from harmless variations in user behavior.



Deep Monitoring and Security

Security Assessment

Sensitive Server and Data Discovery scans the network first for the location of all database, application and Web servers, and then for the sensitive data (credit card numbers, social security numbers, etc.) that exists within those systems. Even encrypted data can be identified and monitored.

SecureSphere uniquely provides three distinct assessment capabilities: sensitive server and data discovery, configuration assessment, and behavior assessment. Together, these capabilities deliver, by far, the industry's most detailed analysis of security and compliance posture. SecureSphere assessment information is presented in easy to understand reports that prioritize risk, support targeted corrective action, and document compliance status.

Configuration Assessment queries the database for compliance with over 500 security tests. Testing covers five key areas including known software flaws, software configuration, privileges, external objects, and compliance.

Behavior Assessment identifies vulnerabilities that can only be identified by monitoring user behavior over time. For example, login events are analyzed over time to detect shared usage of the systems admin account (or any account) by multiple users – a clear violation emphasized by most security frameworks.

Unauthorized Behavior Protection – Imperva's Dynamic Profiling

SecureSphere's Dynamic Profiling technology automatically creates and maintains verified baseline profiles of each user's business activity. Security and compliance staff may compare user profiles to job functions, regulatory requirements, or best

practices. Profiles may then be customized or immediately converted into policies that SecureSphere uses to detect unauthorized behavior and variations from compliance mandates over time. A significant deviation from an authorized profile generates an alert and may be optionally blocked. Consider a direct marketing specialist, who normally pulls data from a customer address table, but then suddenly accesses the credit card table. SecureSphere recognizes this deviation from normal behavior, issues an alert, and may optionally block access.

User Accountability

One of the primary objectives of any security system is validation that user accountability has been established. Unfortunately, when users access database records through business applications (Oracle EBS, SAP, PeopleSoft, custom), user IDs are not sent to the database and therefore cannot be detected by typical database audit, monitoring and security solutions.

SecureSphere's Universal User Tracking technology makes users accountable for their actions – even when they access data through business applications. To identify application IDs, a dedicated SecureSphere interface monitors application user sessions and correlates those sessions with specific database transactions. For example, a SecureSphere-based SOX audit of financial records links specific application user IDs to specific database changes – even if the change is made through a finance application.

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.

Database Platform Protection

SecureSphere's integrated Intrusion Prevention System (IPS) protects against worms and other attacks targeting known vulnerabilities in database server platforms. IPS capabilities include full Snort®-compatible signature dictionaries (all protocols) and proprietary SQL-specific signatures from the ADC. In addition, the industry's only SQL protocol validation capability mitigates risk associated with the increasing number of database protocol exploits.

SecureSphere's integrated stateful network firewall protects against unauthorized users, dangerous protocols, common network layer attacks, and worms. Firewall policies also meet compliance requirements to restrict database exposure to nonessential network traffic.

Sophisticated Attack Detection

Imperva's unique Correlated Attack Validation (CAV) technology correlates violations across security layers and over time to accurately identify the most complex attacks. Certain individual user profile violations, for example, may not definitively indicate attack. However, by correlating unique combinations of profile with signature violations from the same user, attacks are validated beyond a doubt. No other solution can match the accuracy SecureSphere achieves through CAV.

Local Database 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 can be buffered locally to prevent loss in the event of network downtime. Together, SecureSphere agents and appliances ensure complete monitoring of all activity.

Flexible Audit Policy Definition

SecureSphere’s Audit Policy Wizard enables monitoring of all events, or selective event tracking based on a combination of attributes. Audit data extends from high level attributes such as user names, to granular capture of query text, response text, response codes, etc. No other solution matches SecureSphere’s ability to track event detail while scaling across the largest global data centers.

Operational Efficiency

Automated Security Policy

The detection of unauthorized database user behavior requires the creation of detailed baseline profiles. However, it is not cost effective or realistic to expect audit and security staff to create and maintain detailed profiles for each user, or even each group. Profiles may contain thousands of elements and change on a daily basis.

Imperva’s Dynamic Profiling eliminates manual user profile configuration and tuning. SecureSphere applies adaptive learning algorithms to automatically develop and adjust profiles as behavior changes over time. However, administrators have full access to modify or create custom profiles as desired. The final result is a security investment that simultaneously minimizes risk and total cost of ownership.

Transparent Deployment

SecureSphere appliances can be deployed on the network as a transparent inline bridge, an inline router or as an offline network monitor. They require no changes to database software, the network, servers, or applications.

Zero Impact on Database Performance, Administration, or Availability

SecureSphere delivers deep monitoring and security without impacting database performance, administration, or availability. SecureSphere gateways do not consume

database resources, while the host agent only monitors local activity – thus consuming negligible resources. Imperva’s Transparent Inspection technology supports multi-gigabit throughput with sub-millisecond latency. In addition, SecureSphere deployment may be completely decoupled from database administration if desired. Finally, a host of availability options ensure maximum uptime. Options include Imperva’s sub-second IMPVHA (active/active, active/passive), fail-open interfaces, VRRP, STP, RSTP, and offline monitoring.

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 of large enterprise and ASP environments 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.

Separation of Duties

SecureSphere presents database information in a manner that is accessible to non-database administrators. As a result, SecureSphere can be managed by security or compliance personnel to maintain separation of duties between security, audit, and database administration if desired.

Business Relevant Reporting

SecureSphere’s provides the market’s most complete set of compliance reports. This helps accelerate audit, security and compliance against a range of regulations/ best practice frameworks including SOX, HIPAA, PCI, etc. 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 security solution delivers the ability to focus on the audit questions relevant to specific regulatory issues and business applications. In addition to pre-defined reports, SecureSphere’s robust reporting framework provides complete

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.

flexibility in creating custom reports and templates to allow for any unique reporting situations. It also integrates the analytical tools needed to document compliance with relevance to specific business environments.

Extending SecureSphere to Web-based Business Applications

SecureSphere can be extended to secure Web-based business applications with the SecureSphere Web Application Firewall. The Database Gateways and Web Application Firewall can work together to enable advanced protection against external threats. For example, database violations can be correlated with Web violations in real time to defeat SQL injection, parameter tampering and other Web attacks with unparalleled accuracy. The SecureSphere Management Server unifies management of mixed Web and database deployments. Together, these products deliver the market’s only complete audit and security solution for business application data.



SecureSphere is able to fully secure the database as well as the database infrastructure by actively blocking known malicious database attacks

Dynamic Profiling Models Database Usage

Profile Element	Description
Database Objects	All database objects - queries, SQL operations, stored procedures and associated operations, prepared statements, bind variables, tables, system objects
Users	Auditable trail of end-user, application, and administrative activity
Normal Business Activities and Transactions	Prevents use of legitimate privilege for illegitimate purposes
Time of Day and Location	Restricts users to normal work hours and locations
Application/Access Method	Application/Access Method Prevents the use of stolen or abused credentials

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 Network Segments	(2)Bridge; (5)Router, Non-inline	(2)Bridge; (5)Router, Non-inline	(2)Bridge; (5)Router, Non-inline
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

