



SecureSphere® Database Firewall

Protect and Control Your Critical Databases

With real-time protection against internal threats and external attacks, coupled with detailed activity auditing, SecureSphere helps businesses:

- » *Block database attacks and fraudulent activity*
- » *Transparently protect databases through virtual patching*
- » *Leverage flexible views and audit analytics to further investigate audited events*
- » *Automate and centralize database protection*
- » *Complete the data security and compliance lifecycle*

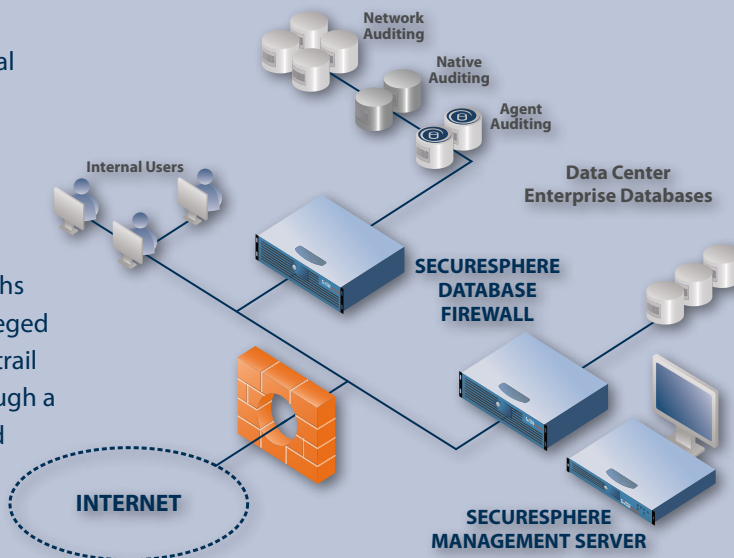
Database Firewall



**Only the market leading
SecureSphere Database
Firewall can actively protect
your critical databases.**

Unmatched Database Protection

SecureSphere Database Firewall provides active protection, virtual patching and complete visibility for all major database platforms including Oracle, MS-SQL, IBM DB2, Sybase, Informix, MySQL and Teradata. Deployed as either inline or non-inline network monitoring appliances, coupled with light weight SecureSphere agents, interfacing with native database auditing tools, or working a hybrid combination, it protects all database access paths and provides visibility into all activity types, including local privileged activity. SecureSphere establishes a detailed, independent audit trail of database activity in a tamper-proof repository, accessible through a Web-based UI (role based access controls enforced). A centralized management server enables unified management of distributed gateways and agents.



The SecureSphere Database Firewall (DBF) solution is designed to provide the industry's best automated protection for critical database platforms. Through real-time activity blocking it controls access to databases and protects against fraud, abuse, and external attacks. Providing complete visibility into database activity enables organizations to implement a complete database security and compliance solution.

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 understand which servers are within the scope of a regulatory compliance project and may require more stringent controls.

Comprehensive Vulnerability Assessment

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

The assessment tests are kept up-to-date with the latest research from the Imperva Application Defense Center (ADC) research team. From the Vulnerability Workbench users can apply Virtual Patching to block exploitation attempts.

Intelligent Behavioral Assessments

Behavioral assessments provide visibility into the ways users and application access and manipulate data stored in databases. By capturing activity details like the user, date and time of the event, source, destination and the tools/ applications used, and building a comprehensive profile, SecureSphere can provide detailed analysis, alert and optionally block abnormal activity.

Database Activity Monitoring Automatic Auditing

SecureSphere includes a complete set of predefined security and audit policies which can be quickly implemented for protecting any database environment. These policies are based on 'Black-list' and 'White-list' security modules which are continuously updated: The 'Black List' is updated by the Imperva ADC research group, the 'White List' is updated by Imperva's patent pending Dynamic Profiling technology, which 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 database objects, users and SQL queries.

Independent Monitoring and Auditing

As an independent security 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.

Tamper-Proof Audit Trail

SecureSphere captures the detailed audit trail that shows the 'Who, What, When, Where and How' of each transaction.

The audit trail is stored in an external, secured and hardened repository which can be accessed through read-only views. To ensure the integrity of the audit trail it can also be signed or encrypted.

Real-Time Database Protection Blocking Unauthorized Activity

Continuous real-time monitoring and analysis of all database operations allows SecureSphere to respond quickly and block unauthorized activities. SecureSphere monitors network and direct access to databases and captures all database

Database Security 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. 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.



Meeting PCI-DSS Requirements:

The PCI-DSS requirements emphasize the importance of real-time monitoring and protection of cardholder data. Out of the 12 requirements, 8 are addressed by SecureSphere DBF, including:

- A built-in firewall to protect and control access to cardholder data
- Built-in assessments confirm that vendor supplied accounts and passwords are not in use
- Monitoring and auditing all access to cardholder data in a tamper-proof audit trail
- Intelligent alerts on unauthorized access to cardholder data
- Measures effectiveness of audit and security controls through built-in and custom reports
- Implementation of a continuous, automated security and compliance lifecycle

SecureSphere enables merchants and service providers to address the most challenging PCI requirements quickly, painlessly, and cost effectively.

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.

Attack Blocking and Virtual Patching

As SecureSphere monitors live database activity it looks for various database attacks at the OS and protocol level as well as the SQL activity level to provide accurate real-time protection. Unauthorized change, fraudulent activity, and database attacks can be blocked on the network before reaching the protected system, or on the system itself.

Virtual Patching helps transparently protect vulnerable systems which can't be patched or modified.

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 monitored 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. 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, Lower TCO

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

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

Performance and Scalability

Unmatched by any other Database firewall solution, SecureSphere provides real-time protection 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. SecureSphere reduces administration and maintenance, and provides a low-cost, effective audit and security solution

Validating and Controlling 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 ensuring full visibility and protection capabilities to 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. SecureSphere DBF protects databases through automated blocking of unauthorized local privileged activities and real-time blocking of network activities, terminating and preventing these activities from taking place on the protected server.

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

Real-Time Protection

Alert and block unauthorized activities and database attacks on the network or directly on the monitored server

Virtual Patching

SecureSphere Virtual Patching for vulnerable servers which can't be patched or modified

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-DBF_0409rev1