



SecureSphere® Data Security Suite

Full Visibility and Control for Applications
and Databases

Delivering end-to-end protection for applications and databases, SecureSphere addresses all aspects of the data security lifecycle. SecureSphere helps businesses:

- » *Protect both applications and databases*
- » *Deliver an independent audit trail and intelligent audit analytics*
- » *Identify the application users that perform database transactions*
- » *Streamline audit and compliance efforts*
- » *Transparently deploy in any environment with zero impact on performance*

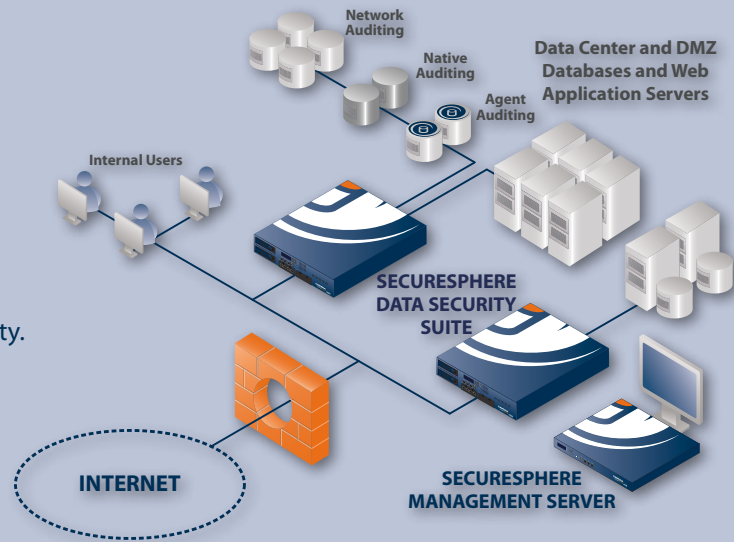
Integrating market leading Web and database security technology, the SecureSphere Data Security Suite sets the standard for data security, auditing, and compliance.



The Industry Standard in Data Security, Auditing, and Compliance.

The SecureSphere® Data Security Suite unifies audit, security, and risk management for business databases and the applications that use them. In a single, comprehensive security platform, the market-leading Web Application Firewall, Database Activity Monitoring, and Database Firewall prevent sensitive data theft, protect against data breaches, secure applications, and ensure data confidentiality.

Combining visibility and control for both applications and databases, SecureSphere delivers full activity monitoring from the database to the accountable application user and is widely recognized for its overall ease of management and deployment.



Trusted Leader in Data Security

With the only solution in the world that protects data from the database, through the application to the end user, Imperva understands that Web and database security together are designed to achieve one ultimate goal: to safeguard sensitive data.

Combining the security of the SecureSphere Web Application and Database Firewalls, the visibility of Database Activity Monitoring, and the vulnerability management of the Discovery and Assessment Server, the SecureSphere Data Security Suite provides a comprehensive risk management framework to assess, audit, and protect the most critical assets in any organization: the database and the business applications that use them.

User Accountability

By unifying Web and database activity monitoring, SecureSphere solves a key requirement for audit and compliance: identifying application end users that performed database transactions, even in multi-tier environments.

SecureSphere's Universal User Tracking discovers application IDs, monitors user sessions and correlates those sessions with specific database transactions. SecureSphere accurately associates application users with SQL queries, enforcing user accountability as mandated by compliance regulations.

Complete Visibility and Control

By providing an integrated solution, organizations gain unmatched insight, accurate identification of end users, and correlation of application and database activity. SecureSphere is the clear choice to assess, monitor, and protect sensitive data.

Discovery and Assessment Server

The SecureSphere Data Security Suite includes the Discovery and Assessment Server, which discovers database servers, classifies database data based on sensitivity level, and assesses databases for vulnerabilities.

To assess organizations' security and compliance posture, SecureSphere scans databases for over 1,000 vulnerabilities and mis-configurations.

All assessment results are presented in easy to understand reports that prioritize risk, support targeted corrective action, and document compliance status.

Optional User Rights Management (URM) add-on provides the ability to aggregate, view, and analyze excessive and dormant user rights on database systems.

Database Activity Monitoring

SecureSphere delivers automated and scalable activity monitoring, auditing, and reporting for Oracle, MS-SQL, DB2, Informix, MySQL, Sybase, SybaseIQ, and DB2/400.

SecureSphere tracks SQL transactions for forensics, prevents database leaks, and ensures data integrity by establishing an independent audit trail of user activity.

Detailed Activity Monitoring

SecureSphere captures all database actions, including DML, DDL, DCL, and read-only activity, as well as changes made to store procedures, triggers, and database objects, ensuring complete audit trails of database activity.

Audit Analytics and Compliance Reports

Visibility into audited activities enables non-technical auditors to analyze, correlate, and view database activity with just a few mouse clicks, uncovering the patterns and trends that indicate security risks. SecureSphere provides both fully-customizable and "out-of-the-box" reports for security and compliance.

Zero Impact on Performance

Unlike native database logging or software auditing, SecureSphere imposes no impact on database or application performance.

Database Firewall

Building on the visibility provided by Database Activity Monitoring, the SecureSphere Database Firewall provides real-time protection to prevent database intrusions, fraud, and sensitive data loss.

Web Application Firewall

The SecureSphere Data Security Suite leverages the power of the market-leading SecureSphere Web Application Firewall to protect applications against sophisticated attacks. SecureSphere accurately blocks SQL injection, Cross-Site Scripting (XSS) and brute force login, stops online identity theft, and prevents data leaks from applications.

Automated Security

SecureSphere's unique Dynamic Profiling technology automatically learns the structure, elements, and usage of protected Web applications. By comparing transactions to the profile, SecureSphere detects malicious activity with pinpoint precision.



Streamline Audit and Compliance

SecureSphere includes pre-defined assessments, audit rules, and compliance reports that enable organizations to jumpstart their audit initiatives and eliminate manual reporting processes.

SecureSphere helps organizations address multiple security and compliance mandates, including PCI, SOX, HIPAA, NERC CIPS, GLBA, and Basel II. SecureSphere has even been certified by ICSA Labs for PCI DSS. With SecureSphere, organizations can automate compliance processes and demonstrate security status to auditors.

Unparalleled Accuracy

SecureSphere performs multiple layers of inspection, detecting:

- » Usage violations by Dynamic Profiling
- » Application attack signatures
- » Reputation-based security with ThreatRadar
- » HTTP protocol violations
- » Network and platform attacks
- » Web services (XML) attacks
- » Session exploits
- » Data leakage signatures

With transparent deployment, automated and up-to-date security, and low operational overhead, SecureSphere is the only choice to protect critical applications and databases.

Addressing the Full Data Security and Compliance Life Cycle

With an increasing number of industry and government regulations, businesses must implement a repeatable process that addresses data governance and data protection. The SecureSphere Data Security Suite empowers organizations to establish a successful framework for security and standards compliance.

Because many regulations are vague and subject to interpretation, organizations have wasted valuable time and expense coordinating separate compliance initiatives. However, even though the number of regulatory mandates is escalating, more and more regulations present common themes.

Imperva has outlined an actionable set of steps that helps organizations meet many of the regulatory requirements that oversee data governance and data protection.

This iterative compliance framework comprises the following four steps:

1. Discover and Assess
2. Set Policies and Controls
3. Monitor and Enforce
4. Measure

Using this framework, organizations can satisfy compliance requirements, as well as align business objectives, implement controls, and ensure robust security.

Discover and Assess

The first step to achieving data security and compliance is to construct an accurate assessment of applications and databases in the network and their security posture.

SecureSphere can discover database servers, classify sensitive information, and assess databases for vulnerabilities and configuration flaws, and present results in both high-level and detailed reports.

Set Policies and Controls

After performing a risk assessment, the next step is to define policies for security and governance.

SecureSphere can set policies automatically based on out-of-the-box audit and security rules and dynamically learned usage patterns. SecureSphere adapts to application and database user changes, policies are always up-to-date.

Custom correlation rules provide granular control over usage policies.

Measure

Clear, comprehensible reports allow organizations to document compliance status to auditors.

SecureSphere's pre-defined reports and robust reporting framework can present business-relevant reports to any audience with ease. SecureSphere can summarize the results of each stage of the security and compliance lifecycle and illustrate the organization's security risk and compliance state.

Monitor and Enforce

To address auditing and compliance mandates, an auditing solution must capture full details of data activity, ensure data integrity, and enforce user accountability.

SecureSphere monitors all Web and database transactions, including privileged user activity by the DBA. SecureSphere enforces separation of duties and stores audit trails in a secure, tamper-resistant repository.

**Data
Security
and
Compliance
Lifecycle**

SecureSphere Features

Databases Supported

- » Oracle, MS-SQL, Sybase, DB2, Informix, MySQL, Teradata, DB2/400

Discovery and Classification

- » Database servers
- » Sensitive data (pre-defined and custom)

Vulnerability Assessment

- » Operating system vulnerabilities
- » Database software vulnerabilities
- » Configuration weaknesses

User Rights Management (URM)

- » Optional add-on for auditing and managing database user rights

Database Security

- » Dynamic Profile of user activity
- » Database attack signatures
- » SQL protocol violations

Web Security

- » Dynamic Profile (White List security)
- » Web server & application signatures
- » Reputation-based security
- » HTTP RFC compliance
- » Normalization of encoded data

HTTPS/SSL Inspection

- » Passive decryption or termination
- » Optional HSM for SSL key storage

Web Services Security

- » XML/SOAP profile enforcement
- » Web services signatures
- » XML protocol conformance

Platform Security

- » Platform intrusion prevention
- » Known and zero-day worm security

Network Security

- » Stateful firewall
- » DoS prevention

Advanced Protection

- » Correlated Attack Validation

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

Signature Updates

- » Automated updates

User Tracking Methods

- » Web Application User Tracking
- » Web to Database User Tracking
- » SQL Connection User Tracking
- » Direct Database User Tracking

Centralized Management

- » MX Server for centralized management
- » Integrated management option
- » Hierarchical management groups
- » Web User Interface (HTTP/HTTPS)
- » Command Line Interface (SSH/Console)

Monitoring

- » SNMP
- » Syslog
- » Email
- » Incident management ticketing integration
- » SecureSphere task workflow
- » Integrated graphical reporting
- » Real-time dashboard

High Availability

- » IMPVHA (Active/Active, Active/Passive)
- » Fail open interfaces (bridge mode only)
- » VRRP
- » STP and RSTP

Deployment Modes

- » Transparent Bridge (Layer 2)
- » Router (Layer 3)
- » Non-inline sniffer
- » Light-weight agents for DB host monitoring
- » Remote agent-less collection of database audit logs



SAP® Certified Integration



Imperva

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

© Copyright 2010, 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-DSS_0110rev2