IMPERVA®

Database Security

Audit and Protect Critical Databases

Products

SecureSphere Database Activity Monitor

SecureSphere Database Firewall

SecureSphere Database Assessment

User Rights Management for Databases

ADC Insights

Best-in-Class Database Auditing and Protection

Databases store extraordinarily valuable and confidential data. An increasing number of regulations compel organizations to audit access to this sensitive data and protect it from attack and abuse.

Award-winning Imperva SecureSphere Database Security products automate database audits and instantly identify attacks, malicious activity, and fraud. Combined with Imperva's Web Application Security and File Security products, Imperva SecureSphere is the premier choice for securing sensitive business data.

Imperva SecureSphere Database Security Products

- Audit all access to sensitive data
- Alert or block database attacks and unauthorized activities in real time
- Detect and virtually patch database vulnerabilities
- Identify excessive user rights and dormant users, and enable a complete rights review cycle
- Accelerate incident response and forensics investigations with advanced analytics

Meet Compliance Requirements

SecureSphere helps organizations address multiple compliance regulations including PCI DSS, SOX, and HIPAA.

- Addresses 8 of 12 high-level PCI requirements, including sections 10, 7, and 8.5
- Meets auditing requirements for financial data in SOX sections 302 and 404
- Enforces separation of duties
- Ensures audit data integrity
- Detects unauthorized access to financial and cardholder data
- Offers pre-defined reports that streamline compliance

Imperva Data Security Capabilities

Continuous Auditing of Sensitive Data Usage

SecureSphere continuously monitors and audits all database operations in real time, providing organizations with a detailed audit trail that shows the 'Who, What, When, Where, and How' of each transaction. SecureSphere audits privileged users who directly access the database server, as well as non-privileged users accessing the database through various applications. SecureSphere also monitors the database response to alert or stop leakage of sensitive data.

Audit Analytics for Incident Investigation and Forensics

SecureSphere provides deep insight into audited activities through interactive audit analytics. SecureSphere enables security teams and database auditors to quickly view, analyze, and correlate database activities from virtually any angle from a simple user interface, without requiring any SQL scripting. Interactive audit analytics simplifies forensic investigations and enables identification of trends and patterns that may indicate security risks.

Detection of Unauthorized Access, Fraudulent Activity

SecureSphere identifies normal user access patterns to data using patent-pending Dynamic Profiling technology. It establishes a baseline of all user activity including DML, DDL, DCL, read-only activity (SELECTs), and usage of stored procedures. SecureSphere detects material variances when users perform unexpected queries and alerts or blocks users who violate access policies. Users performing unauthorized SQL requests can also be quarantined until their access rights have been reviewed and approved.

Real-Time Blocking of SQL Injection, DoS, and More

While selectively auditing access to sensitive data, SecureSphere monitors all database activity in real time to detect unknown data leakage, unauthorized SQL transactions, and protocol and system attacks. Whether originating from an application or a privileged user, on the network or on the database server itself, SecureSphere can alert on and optionally block malicious attacks.

Policy Enforcement, Streamlined Compliance Reporting

SecureSphere includes a complete set of predefined, customizable security and audit policies. Out-of-the-box awareness of enterprise applications such as SAP, Oracle EBS, and PeopleSoft and key regulations including SOX, PCI DSS, and HIPAA simplify deployment and time to compliance. Security alerts can be sent to SIEM, ticketing systems, and other third-party solutions to streamline business processes.

Classifying Data in Scope for Compliance and Security

SecureSphere detects all database systems in scope for security and compliance projects through automated discovery and classification of sensitive data. Combining discovery and classification with vulnerability assessment enables organizations to prioritize vulnerability remediation efforts.

Assessment and Virtual Patching of Database Vulnerabilities

Including over fifteen hundred configuration, database, and platform vulnerability assessments, SecureSphere helps organizations identify and remediate vulnerabilities. For immediate protection, SecureSphere Virtual Patching can block attempts to exploit discovered vulnerabilities. Virtual Patching minimizes the window of exposure and drastically reduces the risk of a data breach while testing and deploying database patches.

Effective User Rights Management Across Databases

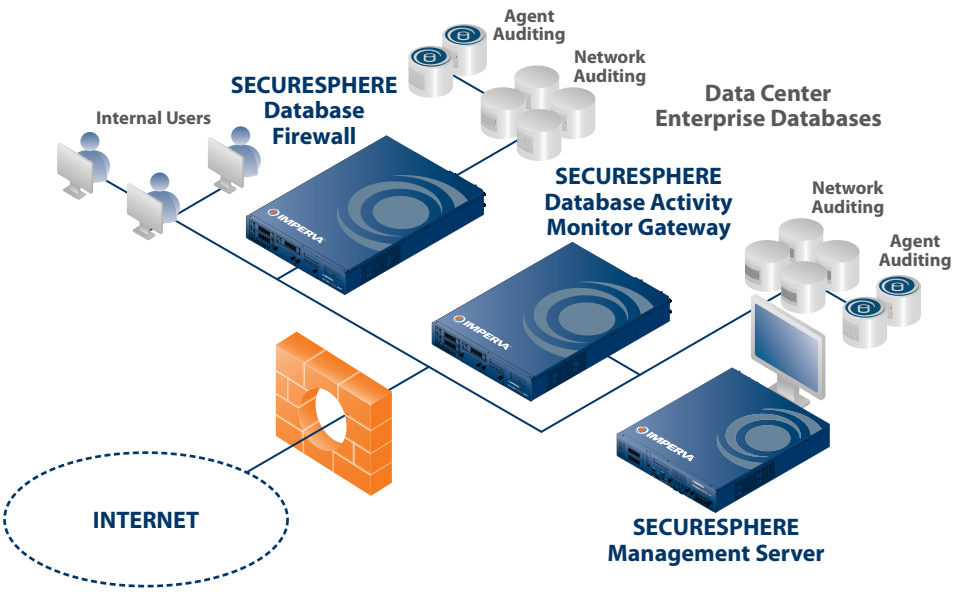
SecureSphere automatically aggregates user rights across heterogeneous databases. With User Rights Management, organizations can establish an automated process for access rights review, identify excessive user rights, and demonstrate compliance with regulations such as SOX, PCI 7, and PCI 8.5.

Local Database Auditing and Protection Using Lightweight Agents

For complete visibility and control of all user activity, SecureSphere extends its monitoring, auditing, and enforcement capabilities to database servers. Lightweight SecureSphere agents audit database activity and protect sensitive data with minimal impact to server performance.

Unparalleled Database Security and Compliance

SecureSphere addresses all aspects of database security and compliance with industry-best database auditing and real-time protection that will not impact performance or availability. With its multi-tier architecture, SecureSphere scales to support the largest database installations. By automating security and compliance, it is not surprising that thousands of organizations choose Imperva SecureSphere to safeguard their most valuable assets.



Deployment

- **Non-inline Network Monitoring.** Activity monitoring with zero impact on database performance or availability
- **Transparent Inline Protection.** Drop-in deployment and industry-best performance
- **Agent-based Monitoring and Blocking.** Lightweight software agents that monitor and block direct privileged activities and network traffic
- **Gateway Clustering.** Cost-effective resilient database auditing
- **Supported Database Platforms.** Oracle, Oracle Exadata, Microsoft SQL Server, IBM DB2 (on Linux, UNIX, Windows, z/OS and DB2/400), IBM IMS on z/OS, IBM Informix, IBM Netezza, SAP Sybase, Teradata, Oracle MySQL, PostgreSQL, and Progress OpenEdge

Imperva SecureSphere Data Center Security

Imperva SecureSphere is a comprehensive, integrated security platform that includes SecureSphere Web, Database and File Security. It scales to meet the data center security demands of even the largest organizations and is backed by the Imperva Application Defense Center, a world-class security research organization that maintains the product's cutting-edge protection against evolving threats.

WEB APPLICATION SECURITY PRODUCTS

Web Application Firewall
Accurate, automated protection against online threats

ThreatRadar Reputation Services
Leverage reputation data to stop malicious users and automated attacks

ThreatRadar Community Defense
SecureSphere deployments around the world provide crowd-sourced threat intelligence to subscribers

ThreatRadar Fraud Prevention
Stop fraud malware and account takeover quickly and easily

Incapsula SaaS WAF and DDoS Protection
Best-of-breed web application security and content delivery as a service

DATABASE SECURITY PRODUCTS

Database Activity Monitor
Full auditing and visibility into database data usage

Database Firewall
Activity monitoring and real-time protection for critical databases

Database Assessment
Vulnerability assessment, configuration management, and data classification for databases

User Rights Management for Databases
Review and manage user access rights to sensitive databases

ADC Insights
Pre-packaged reports and rules for SAP, Oracle EBS, and PeopleSoft compliance and security

FILE SECURITY PRODUCTS

File Activity Monitor
Full auditing and visibility into file data usage

File Firewall
Activity monitoring and protection for critical file data

User Rights Management for Files
Review and manage user access rights to sensitive files

Directory Services Monitor
Audit, alert, and report on changes made in Microsoft Active Directory

SHAREPOINT SECURITY PRODUCTS

SecureSphere for SharePoint
Visibility and analysis of SharePoint access rights and data usage, and protection against web-based threats

IMPERVA®

www.imperva.com