IMPERVA®

SecureSphere Database Activity Monitoring and Database Firewall

DATASHEET

SecureSphere provides:

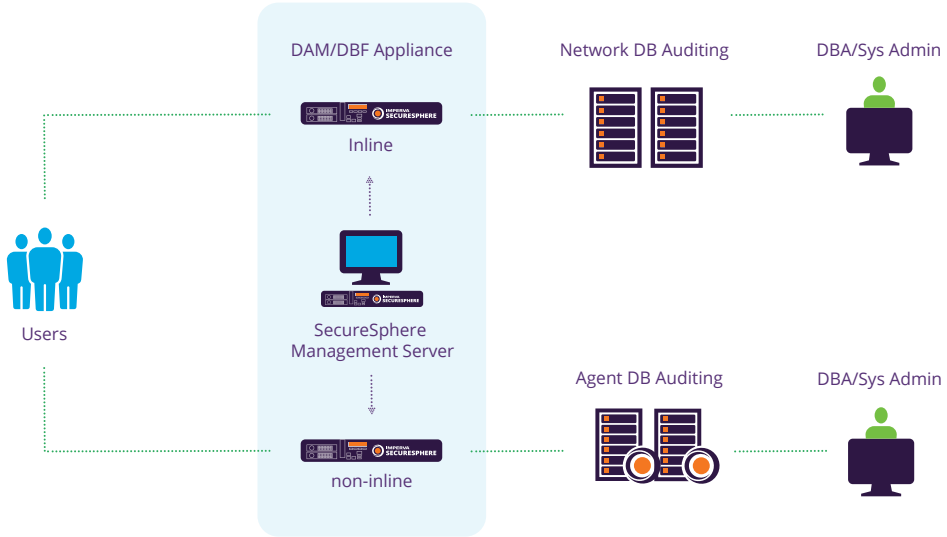
- Database discovery
- Data classification
- Database vulnerability assessment
- User rights management
- Database activity monitoring
- Compliance audit reporting
- Policy enforcement and event blocking

Discover sensitive data, identify vulnerabilities, monitor database user and privileged account activity, protect against data breach, and gain a clear actionable picture of compliance and security status.

Best-in-class solution with rapid time to value

Imperva SecureSphere for database provides a database monitoring and audit solution that satisfies a broad range of compliance requirements - while also providing real-time data protection - with little or no adverse impact on database performance.

SecureSphere quickly delivers a positive return on investment by centralizing database audit and protection across heterogeneous enterprise systems, automating processes and making them easily repeatable, while reducing the amount of resources needed to achieve database risk management goals.



SecureSphere monitors database activity for both privileged and application user accounts

Centrally manages Database Audit and Protection across traditional on-premises relational databases, big data platforms, and cloud database services.

Extend protection by detecting dangerous access behavior

Imperva CounterBreach, which integrates with SecureSphere, enables organizations to extend data protection by intelligently assessing complex user behaviors that could be leading risk indicators. By using machine learning and peer group analytics, CounterBreach compares daily database activity to a longer term contextual baseline and pinpoints activity that is risky or might indicate a breach.

Establish enterprise-wide coverage

SecureSphere helps organizations address regulations such as GDPR, PCI-DSS, SOX, POPI, HIPAA and others by automating discovery and classification of sensitive data, assessing database vulnerabilities, recording database account activity, and producing compliance audit reports – at enterprise-class performance and scalability – across traditional RDBMS, Big Data architectures, and cloud database services.

Data support includes dozens of enterprise relational database and Big Data platforms such as Oracle, Microsoft SQL, IBM DB2, Sybase, Informix, Teradata, Postgres, SAP-HANA, Hadoop, MariaDB, MongoDB, Cassandra and more. Cloud-hosted database services from vendors such as Amazon and Microsoft are also supported – including Amazon's Relational Database Service (RDS).

Discover databases and sensitive data sources

As the size of a company grows, so grows the number of databases, and the amount of sensitive data that is accumulated. SecureSphere uses automated procedures to locate database servers and pinpoint sensitive data, then can classify the data to help companies plan their risk mitigation programs, systems, and policies.

Continuous monitoring with separation of duties

SecureSphere captures and analyzes all database activity, from both application user and privileged user accounts, providing detailed audit trails that shows the "Who, What, When, Where, and How" of each transaction – and is separately administered from the database – ensuring the audit trail meets regulatory guidelines and standards of trust. Monitoring can be done by either network probes or host-based agents.

Security policy enforcement

Monitoring for security and compliance policy is done in separate but parallel channels – enabling SecureSphere to cache high fidelity audit data while still looking at security information in real-time. Other database monitoring solutions that don't use separate compliance and security channels aren't able to respond quickly to security violations.

Detecting attacks in real-time is the only effective way to prevent hackers from getting your data. SecureSphere uses the security channel to look for attacks on network protocols, operating systems, as well as application layer SQL activity - and can quarantine activity pending user rights verification or block the activity - without disrupting business by disabling the entire account. Blocking is available through both database agents and network appliances.

Predictable performance and availability at scale

Imperva delivers enterprise-wide scalability through fault tolerant architecture and highly efficient audit logging technology. Unlike competing solutions, which rely on standard relational databases to record monitoring activity, Imperva utilizes logging techniques found in big-data analytics solutions. The unique ability of SecureSphere to write fast, and read even faster, gives it the ability to scale far beyond the competition.

SecureSphere eliminates single points of failure with active redundancy, clustering, and agent connections that can balance themselves and move around clusters as needed, thus helping to maintain a fault-free system with uninterrupted visibility.