Imperva SecureSphere Data Security

DATASHEET

Protect and audit critical data

The connectivity and ease of internet access have spawned entirely new forms of cyber-crime. The results are changing how consumers, businesses, and governments view the responsibility of protecting sensitive data. In addition to the actual investigation cost, compliance fines and potential brand damage, there is a new concern. A recent appellate court ruling[1] marked a change in the definition of "customer damage", granting class action status to consumers whose personally identifiable data was stolen during the breach. The company liability as a result of a data loss incident has the potential to increase exponentially as the definition of damage is expanded, and legal costs and settlements mount.

The company liability as a result of a data loss incident has the potential to increase exponentially, as legal costs and settlements mount

Best-in-class data protection and auditing

Imperva is the premier choice for securing sensitive business data and applications in the cloud and on-premises. SecureSphere data protection solutions address all aspects of database security and compliance with best-in-the-industry 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 and Big Data installations. By automating security and compliance, it is not surprising that thousands of organizations choose Imperva SecureSphere to safeguard their most valuable assets.

[1] 7th Circuit Court of Appeals, Judge Diane Wood, Plaintiff Win Victory Regarding Neiman Marcus Data Breach

Imperva SecureSphere for data

- Discover and help classify sensitive databases
- Identify excessive user rights and dormant users, and enable a complete rights review cycle
- Protect RDBMS, data warehouses, Big Data platforms, and mainframe databases
- Alert, quarantine, and block database attacks and unauthorized activities in real-time
- Automate and schedule compliance tasks and reporting

Protect data at the source

SecureSphere data security monitoring and independent audit logging for compliance

- Log only what activity is necessary while monitoring all activity for security violations
- Monitor and protect high-transaction databases
- Block suspicious behavior when it happens – investigate in-context
- Execute multi-action security alerts, eliminating bottlenecks and delays
- Interlock database protection with the SecureSphere Web Application Firewall, Account Take-over Protection, and malware protection, providing multi-factored data security

Meet compliance requirements

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

- Addresses virtually all compliance requirements for databases with pre-defined policies and reports
- Rapid configuration and deployment of new and modified policies – no DBA required
- Enforced separation of duties with tamperproof audit data
- In-service and phone home updates minimize restarts and resulting gaps in audit data
- Flexibility and responsiveness to address evolving IT environments and compliance requirements

Data protection and audit is a company-wide necessity

Hackers and data thieves don’t care who “owns” data security or compliance within a company – their intent is to steal data for personal gain. The use of multi-vector attacks illustrates how they can use team and system silos to circumvent security. A DDoS attack distracts, while another vector of the attack utilizes compromised user credentials, obtained via a spear phishing email and malware, to steal thousands of data records. Stopping the data theft is not feasible with manual monitoring and stand-alone security measures. Correlated security dashboards help, but when alerts flood the system, the “real” attack may go unnoticed for weeks or longer. Proactive security monitoring deployed at the data level is the last opportunity to stop an in-progress data attack. When integrated with a web application firewall, anti-malware solutions and other security measures, the odds of keeping data secure shift in the company’s favor. Data thieves thwarted; the IT, security, and compliance teams can reflect that together they achieved their overlapping objectives of keeping data safe and demonstrating that they are doing it in accordance with compliance mandates and regulations.

SecureSphere Database Assessment pinpoints sensitive data locations and provides a risk-based prioritization that can help companies plan their risk mitigation programs, systems, and policies

Imperva data security capabilities

Data security starts with data discovery

To protect and monitor data in requires the discovery and classification of the sensitive data. In smaller companies this may be achieved through manual surveys and reviews; as the size of a company grows, the number of databases grow at a near-exponential rate. Automated discovery and classification are the only reliable way to routinely and consistently discover and classify new or modified database instances containing previously unknown sensitive data. SecureSphere Database Assessment pinpoints sensitive data locations, and provides a risk-based prioritization that can help companies plan their risk mitigation programs, systems, and policies.

Continuous monitoring of sensitive data usage

Even with a high volume of database traffic, SecureSphere simultaneously monitors all traffic for security policy violations and compliance policy purposes. The highly efficient monitoring for separate purposes allows companies to address both security and compliance requirements with a single unified solution.

SecureSphere analyzes all database activity in real-time, providing organizations with a proactive security enforcement layer and 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 users accessing the database through a browser, mobile, or desktop-based application.

Monitor Big Data, SharePoint, and files stores

While databases remain a prime target for cyber theft, sensitive data exists across the enterprise in many types of systems. SecureSphere automates the most challenging aspects of uniform policy deployment and monitoring across databases, Big Data, SharePoint and file stores.

- SecureSphere Agent for Big Data extends SecureSphere Data Activity Monitor to leading Big Data offerings including MongoDB, Cloudera , IBM BigInsights, and Hortonworks products.
- SecureSphere File Security products deliver real-time file monitoring, auditing, security, and user rights management for files stored on SharePoint, file servers, and network attached storage (NAS) devices.

Unlike solutions that require DBA involvement and reliance on expensive professional services, SecureSphere provides the necessary management and centralization capabilities to manage thousands of databases, Big Data nodes, and file repositories.

Detection of unauthorized access, fraudulent activity

SecureSphere identifies normal user access patterns to data using Imperva patented Dynamic Learning Method (DLM) and Adaptive Normal Behavior Profile (NBP) 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 triggering further investigative or blocking action.

Multi-action alerts, temporary quarantines and - if appropriate - blocking of unauthorized activities can be used to protect data without the need to disable the user's account, avoiding potential disruptions in critical business processes. Automated remediation workflows drive multi-action security alerts that can send information to SPLUNK, SIEM, ticketing, or other third-party solutions to streamline any broader investigation processes.

Unified policy deployment and enforcement

Another advantage of SecureSphere is the built-in subject matter expertise. Many organizations struggle to maintain sufficient in-house resources that have the pre-requisite skill set required for deploying and operating a sophisticated data-centric security and audit system. A successful implementation of access controls and audit processes requires making them repeatable. Centralized management of audit and assessment of heterogeneous systems simplifies the management of these processes, while automation reduces the amount of resources needed to maintain compliance, and provides a positive return on investment.

Unlike solutions that require DBA involvement and reliance on expensive professional services, SecureSphere provides the necessary management and centralization capabilities to manage thousands of databases, Big Data nodes, and file repositories. Pre-defined policies, remediation workflows, and hundreds of reports markedly reduce the need for SQL scripts and compliance matter expertise. Elimination of the need for on-going DBA involvement ensures compliance with the separation of duties requirement. By utilizing the of out-of-the-box process API's, management console, workflows, reports and analysis tools, existing personnel can deploy, and manage the system.

Streamlined compliance reporting

Imperva SecureSphere includes hundreds of pre-defined reports addressing the most requested needs of our clients. Additionally, the solution includes a custom report writer for enterprise-specific reporting requirements. Embedded workflows and automation ensure compliance tasks and reporting is done on-time across the entirety of the data set.

Stopping attacks in real-time is the only effective way to prevent hackers from getting to your data. SecureSphere DAM monitors all traffic for security policy violations, looking for attacks on the protocol and OS level, as well as unauthorized SQL activity

Effective user rights management across databases

Virtually every regulation has requirements to manage user rights to sensitive data. Complying with these requirements is one of the most difficult tasks for enterprises to manually perform across large data sets. SecureSphere automatically aggregates user rights across heterogeneous data stores, and helps establish an automated access rights review process to eliminate excessive user rights. It facilitates a routine demonstration of compliance with regulations such as SOX and PCI DSS. The automation of these mundane, but critical tasks, lowers labor costs and reduces the risk of error or reporting gaps.

Real-time blocking of SQL Injection, DoS, and more

Stopping attacks in real-time is the only effective way to prevent hackers from getting to your data. SecureSphere monitors all traffic for security policy violations, looking for attacks on the protocol and OS level, as well as unauthorized SQL activity. The highly efficient monitoring can quarantine activity pending user rights verification or block the activity – without disrupting business by disabling the entire account.

Blocking is available both at the database agent and network levels enabling the fine tuning of the security profile to balance the need for absolute security with the need for performance on critical high-transaction databases.

To truly enhance proactive security, deploy Imperva SecureSphere Web Application Firewall, which utilizes the same architecture and management platform as SecureSphere data solutions. Additional integrations with malware protection, SIEM, and other specialized security systems help organizations align processes and close security gaps.

Audit analysis for incident investigation and forensics

Imperva SecureSphere provides a unified solution enabling independent functional operations while connecting the dots for the security, compliance, and legal teams during an investigation. Imperva provides access to both historical and real-time data, giving incident response teams accurate and contextual visibility into activity as it is happening. The real-time capability, user tracking, remediation workflows, correlation with SecureSphere WAF, and a large number of pre-defined compliance and forensic reports, are all key differentiators for Imperva.

Deployment and configuration automation is a primary factor in time-to-value

An Imperva customer was able to deploy to over 69,000 databases in the span of just a few months using the automation tools

Imperva enterprise-class readiness

Predictable performance at scale

Imperva achieves unmatched scalability through highly efficient audit logging technology. Unlike competing solutions that rely on SQL databases for the data monitoring storage, Imperva utilizes techniques found in the most technologically advanced big-data analytics solutions. The ability to write fast and read even faster gives Imperva the ability to scale far beyond the competition and provides a unique advantage in the marketplace.

The system may be configured to monitor all activity for security policy violations while monitoring and logging a different set of activities for audit purposes. The separation can result in a substantial improvement in data security, performance, audit log size, and relevance when compared to other solutions.

SecureSphere supports high-availability by eliminating single points of failure with active redundancy built into the solution. SecureSphere implements the most advanced and intelligent high-availability features, including exciting new capabilities such as agents that can balance themselves and move around as needed thus helping to maintain a fault-free data protection program ,as well as an uninterrupted audit log.

Rapid deployment

Imperva takes a comprehensive view of the enterprise with a centralized management console capable of providing command and control at a global level. The top-level management console enables the rapid deployment of global policies and automation of tasks such as data classification, thereby speeding implementation time

Imperva also recognizes the value of IT provisioning, providing API sets to facilitate seamless software distribution, configuration updates, policy distribution and data discovery. Deployment and configuration automation is a primary factor in time-to-value. As an example, an Imperva customer was able to deploy to over 69,000 databases in the span of just a few months using the automation tools.

Hybrid monitoring

Imperva goes beyond the typical deployment scenario where agents are required on all database servers; SecureSphere supports multiple deployment methods, including a local agent, a network transparent bridge option, and a non-inline sniffer mode. By using a combination of deployment methods, the enterprise can meet a wide variety of needs without being locked into a single “one-size fits all” model.

Imperva includes the capability to look at the environment and match it to known vulnerabilities providing a clear picture of exactly what data is at risk

Cloud-enabled

Imperva SecureSphere for AWS extends the security and compliance capabilities of the world's most trusted and scalable data protection and audit solution to the Amazon Web Services environment. SecureSphere is the only enterprise-class data protection and compliance solution available for AWS. Running natively in the AWS, the BYOL version of SecureSphere leverages the same market-leading capabilities as the on-premise version. Clients deploying any of the SecureSphere solutions (DBF, DAM, or WAF) in the AWS environment may optionally enable Imperva SkyFence for protection of their cloud-based web applications like Office 365 and the AWS Management Console.

Assessment and virtual patching of database vulnerabilities

With the enterprise data being stored around the world in a variety of databases, each at a potentially different release and patch level, it is imperative to have a simplified way to seek out known vulnerabilities. Imperva includes the capability to look at the environment and match it to known vulnerabilities, providing a clear picture of exactly what data is at risk. SecureSphere virtual patching blocks attempts to exploit specifically known, but unpatched vulnerabilities. Virtual patching helps minimizes the window of exposure, and drastically reduces the risk of a data breach while testing and deploying database patches.

Rapid time to value

The flexible SecureSphere architecture enables growth without disruption to the existing environment, and allows businesses to do more with less. Imperva brings efficient, predictable enterprise scalability to the table. Recently a Fortune 500 company switched to Imperva because they were unable to plan or budget confidently for the future with their existing solution. With Imperva, the company was not only able to significantly reduce the monitoring footprint and operational costs, but they were also able to plan and budget accurately for their future growth.

Imperva SecureSphere Cyber 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 Imperva Application Defense Center, a world-class security research organization that maintains the product's cutting-edge protection against evolving threats.

	SECURESPHERE DATABASE FIREWALL (DBF)	SECURESPHERE DATABASE ACTIVITY MONITORING (DAM)	SECURESPHERE DATABASE ASSESSMENT (DAS)
Discovery & Classification	Yes	Yes	Yes
Monitor & Audit Log	Yes	Yes	-
Block in Real-Time	Yes	No	-
Vulnerability Assessment[1]	Yes	Yes	Yes
Database Agents[1]	Yes	Yes	-
Gateway Clustering	Optional	Optional	-
Big Data Monitoring	Optional	Optional	-
User Rights Management[2]	Optional	Optional	Optional[3]
Extended Application Specific Service (Oracle, EBS, SAP, Peoplesoft)	Optional	Optional	-
High Availability for Mangement Server (MX)	Optional	Optional	-
Available on Amazon Web Services (AWS) BYOL[4]	Yes	Yes	-

[1] Number included varies by appliance purchase, see SecureSphere Appliances data sheet for details

[2] User Rights Monitoring is not available on Big Data Nodes

[3] Features that require audit log detail will not be available if DAS is deployed stand-alone

[4] Not all options are available in the AWS environment

 DS-SecureSphere-Datbase-Security-091015-rev1