IMPERVA®

Imperva SecureSphere Data Security

DATASHEET

Protect and audit critical data

Keeping pace with the threat of cyber security attacks and the increasingly stringent data protection and privacy regulations is hard. For some IT and security teams, the budget and staff necessary to implement effective security measures are not available due to other business priorities. While executives and Boards are increasing aware of the risks, the reality is that budgets will always require teams to do more with less. IT and Security managers need a data protection solution that delivers security, compliance and a clear business justification. Imperva CounterBreach and SecureSphere Database Firewall monitor data and users, intelligently identify and prioritize risks and presents a clear actionable picture of the risks discovered and stopped. This paper will focus specifically on the SecureSphere Database Firewall (DBF) product family.

Imperva CounterBreach and SecureSphere Database Firewall provide data security, simplified compliance and a clear business justification

Best-in-class data protection and auditing

Imperva is the best choice for securing sensitive business data and applications in the cloud and on-premises. SecureSphere Database Firewall satisfies a broad range of database compliance requirements while providing reliable protection with little or no impact on database performance or availability. The solution's multi-tier architecture scales to support the largest database and Big Data installations. By automating security and compliance tasks, thousands of organizations have simplified their audit process and improved their data protection.

Imperva SecureSphere Database Firewall

- Discover and help classify sensitive databases and data
- Find and remediate database and system vulnerabilities
- Identify excessive user rights and dormant users, and enable a complete rights review cycle
- Protect RDBMS, data warehouses, Big Data platforms, and mainframe databases and files
- 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 use two monitoring channels – one for security policies and one for audit policies. The independence enables resource and task optimization that is not possible with a single channel.

SecureSphere Database Firewall

- Logs only what activity is necessary while monitoring all activity for security violations
- Monitors and protects high-transaction databases
- Blocks suspicious behavior when it happens – investigate in-context
- Executes multi-action security alerts, eliminating bottlenecks and delays
- Interlocks database protection with the SecureSphere Web Application Firewall, CounterBreach Insider threat protection, and malware protection, providing multi-factored data security

Meet compliance requirements

SecureSphere helps organizations address compliance regulations including GDPR, PCI DSS, SOX, POPI, 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
- Privileged user monitoring, including local server access
- 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 Discovery and 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 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 Discovery and Assessment Server (included with DBF and available as a stand-alone server) 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 dual channel 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, z/OS, and files

While databases remain the 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 storage systems.

- SecureSphere Agent for Big Data extends SecureSphere Data Activity Monitor to leading Big Data offerings including MongoDB, Cloudera, Cassandra, IBM BigInsights, and Hortonworks products.
- SecureSphere Agent for z/OS extends SecureSphere classification, monitoring and blocking capabilities to the z/OS mainframe database and file environments.
- SecureSphere File Firewall delivers real-time file monitoring, auditing, and ransomware protection for files stored on 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 files.

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), failed events 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 profiled 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 business processes.

Detect and contain insider threats

Protect enterprise data from theft and loss caused by compromised, careless or malicious users by seamlessly integrating the SecureSphere activity log with Imperva CounterBreach. CounterBreach uses machine learning and peer group analytics to establish a full contextual baseline of typical user access to database tables, and then detects and prioritizes anomalous activity. A dashboard of actionable results explain the issues, possible ramifications, and prioritize them. Once dangerous behaviors are identified, enterprises can quickly quarantine risky users in order to protectively prevent or contain data breaches.

The CounterBreach algorithms are specifically built for analysis of SecureSphere logs. This differs from the generic algorithms utilized by SIEM tools that must normalize logs fed to it from multiple sources. CounterBreach has other advantages over SIEM based user behavior analytics, including access to the complete log of activity. Most SEIM tools are provided with database activity logs that are pre-filtered by defined policy rules designed to either remove the “normal” system activity or alert only on known suspicious behavior. By pre-filtering the baseline data, the algorithm will be incapable of defining “normal” or completing an accurate pattern analysis. The direct connection between SecureSphere and CounterBreach ensure that all activity is analyzed in full context.

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 security and audit systems that rely on scripts and custom development. 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 files. 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

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

DBA involvement ensures compliance with the separation of duties requirement. By utilizing the of out-of-the-box capabilities, 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.

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 evaluates 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 GDPR, 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 traffic for security policy violations, looking for attacks on the protocol and OS level, as well as unauthorized SQL activity. SecureSphere 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.

Imperva SecureSphere Web Application Firewall and SecureSphere File Firewall extend the protection to include web applications and protection from file ransomware. Additional integrations with malware protection, including FireEye, 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 many pre-defined compliance and forensic reports, are all key differentiators for Imperva.

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

Automated health monitoring capabilities detect configuration problems and system errors, thereby reducing administrative overhead and down-time

Dedicated Splunk app for database activity analysis

SecureSphere provides standard integration with a wide variety of SIEM products including ArcSight, QRadar, and Splunk. In version 11.0 Imperva introduced a dedicated API set for Splunk enabling users to add custom activity feeds to their Splunk security dashboards and reports. With the release of the free Imperva Database Activity Analysis Application for Splunk, SecureSphere users have a pre-built dashboard and report set optimized for analyzing SecureSphere database alerts and logs. The deployment requires no Splunk development experience and users may create customized reports using the pre-built reports as templates.

Imperva Enterprise-Class Readiness

Predictable performance at scale

Imperva achieves scalability through highly efficient audit logging technology. Unlike competing solutions that rely on standard relational databases for the data monitoring, Imperva utilizes techniques found in big-data analytics solutions. The ability to write fast and read even faster gives Imperva the ability to scale far beyond the competition.

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 intelligent high-availability features, including agent connections that can balance themselves and move around the Gateway cluster as needed, thus helping to maintain a fault-free data program and uninterrupted audit log.

Rapid deployment and on-going system health monitoring

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

Automated health monitoring capabilities detect configuration problems and system errors which reduce administrative overhead and down-time.

Imperva also recognizes the value of IT provisioning, providing API sets to facilitate seamless software distribution, configuration updates, policy distribution and data discovery.

Hybrid activity 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 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 premises version.

SecureSphere provides protection for databases deployed in the Microsoft Azure cloud environment using the standard SecureSphere Database Agents.

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 specific 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.

The new Imperva RiskSense Vulnerability Manager enables efficient workflow management and mitigation of database vulnerabilities discovered using the Imperva Discovery and Assessment Server (DAS).

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 predictable enterprise scalability to the table. 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.