



## SecureSphere® Discovery and Assessment Server

Know your Database Landscape and Risks

Discovery and Assessment Server

*Understanding the location, type, and risks to database data is the foundation of good data security. SecureSphere helps businesses:*

- » *Discover databases over the network*
- » *Classify database contents*
- » *Assess platform, software, and configuration vulnerabilities*
- » *Measure risks to databases and their contents*
- » *Build a vulnerability management lifecycle*

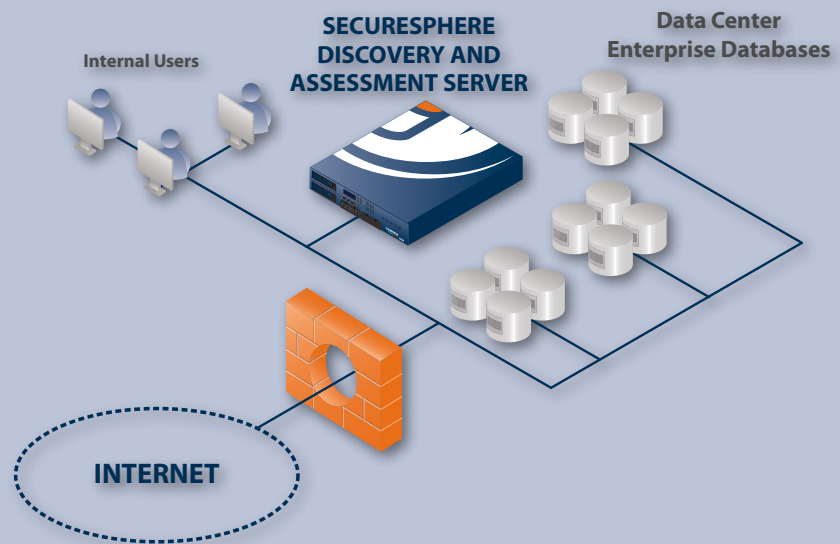


**Only SecureSphere delivers a risk-based approach to database vulnerability management.**

## Discovery, Assessment, and Risk Management

Imperva SecureSphere Discovery and Assessment Server provides organizations with an easy and effective way to implement database vulnerability management through discovery of data assets, classifications of the data they store, and comprehensive vulnerability assessments that identify mis-configurations and potential exploits.

SecureSphere Discovery and Assessment Server enables organizations to establish repeatable automated processes and eliminate cumbersome disparate manual processes. In addition, it provides a unique graphical Risk Explorer that provides critical views and analysis for recognizing risks and prioritizing security and compliance activities.



## Discovery and Classification

### Discovering Databases

An essential part of any compliance and database vulnerability management program is a clear knowledge of the assets requiring protection. The SecureSphere Discovery and Assessment Server (DAS) offers automated network-based database discovery. Scheduled scans of designated networks discover new database installations and ensure awareness of these assets. The discovery results include detailed information about the specific platforms and RDBMS, which combined with data classification and vulnerability assessment and mitigation enable risk management that maps sensitive data with vulnerability risks. Database discovery also helps with asset management and is an important first step for ensuring that rogue database servers do not exist on the network.

### Data Classification

Classifying the data contained within databases helps security and compliance managers to fundamentally understand which databases are within the scope of a regulatory compliance project. SecureSphere uses Dictionaries and Rules as key data classification methods to scan the contents of databases. An extensive list of pre-defined data classification types is included in the solution, and custom data types can be added as well. Asset discovery and data classification scans can be scheduled and repeated to ensure ongoing awareness of types of data within an organization's databases.

### Data Classification Types

SecureSphere DAS offers an extensive list of built in data types in the following classification categories:

- » Financial Information
- » Credit Card Numbers
- » System and Application Credentials
- » Personal Identification Information
- » Custom Data Types

### Discovery and Classification Results

Once discovered and classified, organizations can quickly view discovered platforms and add them to server groups based on location, type of database, and data by classified type. Server groups are then applied with assessment policies. This enables organizations to have full visibility of the data within their organizations. In addition, discovered servers can be added to a server group and included in assessment scans and on-going monitoring.

## Database Vulnerability Assessment

SecureSphere DAS identifies and quantifies vulnerabilities using over 1,000 tests for various platforms and databases. Operating Systems and RDBMSs are tested for known exploits and mis-configurations. Custom assessments can also be added to address specific requirements.

The assessment tests are kept up-to-date with the latest research from the Imperva Application Defense Center (ADC) research team. The ADC team conducts primary research on the latest OS, database and

application vulnerabilities and exploits, and translates the findings into useful assessment tests and signatures. The updated assessments are automatically sent to the SecureSphere systems ensuring up-to-date identification of known vulnerabilities and the ability to protect systems against the latest attacks.

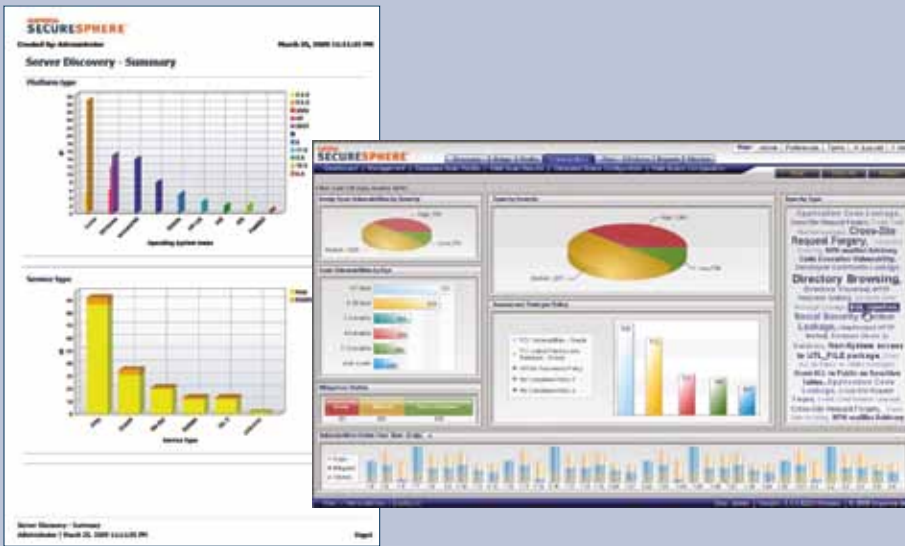
## Database Vulnerability Assessments

SecureSphere DAS arms organizations with a comprehensive list of predefined assessment tests, which is continuously updated by the Imperva Application Defense Center (ADC) research team, providing the most extensive database discovery and assessment solution.

SecureSphere assessments address PCI DSS, SOX, and HIPAA requirements and include the following:

- Latest patches and releases installed
- Changes to database files
- Default accounts and passwords
- Newly created/updated logins
- Remote OS authentication enabled
- Escalated user privileges granted

Additional vulnerabilities specific for SAP, Oracle EBS, and PeopleSoft databases are available with Imperva ADC Insights.



## Vulnerability Analysis and Management

*SecureSphere Discovery and Assessment Server includes analysis views and reports to help manage and mitigate discovered vulnerabilities quickly and efficiently. A Vulnerability Dashboard shows an overview of open vulnerabilities, trends, and mitigation status. An interactive tag cloud depicts vulnerabilities using font size and boldness to indicate the severity and occurrences of each vulnerability. The tags are hyperlinked to analysis views that focus on specific vulnerabilities, allowing users to quickly focus and analyze these vulnerabilities. In addition, automated reports can be easily created from any view and scheduled to send requested information in a PDF or CSV format.*

### Managing Database Vulnerabilities

To assist organizations with tracking and understanding their vulnerabilities, discovered vulnerabilities are assigned with a severity based on the Common Vulnerability Scoring System (CVSS). They are also mapped to a CVE identifier and the NIST standard, allowing users to search and learn more about the vulnerability.

### Mitigating Discovered Vulnerabilities

An interactive vulnerability dashboard helps organization understand and analyze vulnerabilities by showing status, top vulnerabilities, and trending charts with drill down capabilities.

SecureSphere also provides a Vulnerability Workbench where users can track, manage and mitigate discovered vulnerabilities. When deployed with SecureSphere Database Firewall or Data Security Suite it enables vulnerability mitigation through virtual patching and blocking capabilities.

### Effective Data Risk Management

#### Data Risk Explorer

Though for most organizations Risk Management is a top priority, it is often implemented as disparate efforts and manual processes that provide only limited visibility and incomplete analysis. SecureSphere delivers a unique data risk management approach that centralizes and automates data risk management processes and gives better visibility into risks to sensitive data.

The graphical Risk Explorer helps organizations effectively understand the areas of risk in the organization by geographical location, server groups,

servers, and by classified data type. The views support drill down capabilities that provide more details on specific vulnerabilities, supporting quick focus and decision making.

### Audit and Change Management

Pre-defined and custom reports provide detailed visibility into configuration changes, allowing auditors and management to track risk mitigation efforts. Reports are also useful for change management as they can list the configuration changes that take place in the monitored environment. SecureSphere DAS supports integration with SIEM, Workflow, and Ticketing systems.

### User Rights Management (URM)

URM is an add-on option to SecureSphere DAS which provides the ability to aggregate, view, and analyze user rights on database systems. URM enables enterprises to:

- Audit user rights over sensitive data objects
- Document user rights across multiple database systems
- Investigate and correct excessive user rights
- Find dormant user accounts

With URM, organizations are provided with detailed information about user rights which supports the rights approval processes.

### Data Governance and Protection

SecureSphere DAS ensures that organizations are aware of what data is stored in their organization and what steps should be taken to secure it. Dashboards and reports help provide a risk-based view into database vulnerability management. Through centralized management and automated compliance reporting, SecureSphere DAS provides a critical part of any risk, governance, and compliance project.

### Deploying SecureSphere DAS

The SecureSphere DAS is provided as a turn-key network appliance or a virtual appliance:

#### Enterprise Edition

Designed for larger enterprises, with extended platform options. Upgrade paths supported to SecureSphere DAM, DBF and DSS. Supports integration with 3rd party enterprise solutions including SIEM, Workflow, and Ticketing systems.

#### Standard Edition

Designed for medium enterprises looking for a cost effective stand-alone database vulnerability management solutions.

#### DAS Virtual Appliance

Provides the same Discovery, Classification, and Assessment capabilities without a need to deploy a physical appliance. Based on VMware, DAS virtual appliance can be deployed on existing hardware including laptops, desktops, and VMware ESX servers.

## SecureSphere Discovery and Assessment Server - Features and Appliance Specifications

### Coverage

- » Oracle, MS-SQL, Sybase, DB2 (LUW and z/OS), Informix, MySQL

### Deployment

- » A turn-key network based appliance or virtual appliance

### Automated Discovery

- » Automated discovery of database servers and services: IP, ports, database version

### Data Classification

- » Predefined classification policies for financial data, credit card numbers
- » Personally identifiable information, Social Security numbers
- » PCI Prohibited Data (CVV, PIN)
- » Credentials (passwords and usernames), custom data types can be added

### Vulnerability Assessment

- » Operating System vulnerabilities
- » Database vulnerabilities
- » Configuration flaws
- » Risk scoring and mitigation steps

### Assessments for Enterprise Application

- » SAP
- » Oracle E-Business Suite
- » PeopleSoft

### Assessment Polices for compliance with:

- » PCI DSS
- » SOX
- » HIPAA
- » DISA STIG
- » NIST
- » CIS Benchmark

### User Rights Management (URM)

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

### Risk Management

- » Graphical Data Risk Explorer for analyzing risk to data across enterprise assets

### Scheduling

- » Ad-hoc and/or scheduled

### Workflow Actions

- » Accept in scope
- » Reject out of scope
- » Group by site or category
- » Inventory export/import

### Assessment Updates

- » Automated Application Defense Center updates for latest vulnerabilities

### Performance Overhead

- » Non-intrusive network based assessments scans

### Management

- » Web User Interface (HTTP/HTTPS)
- » Command Line Interface (SSH/Console)

### Role-Based Controls

- » Flexible role-based management and delegation of operations and report viewing privileges

### Reports

- » Management summary and detailed results
- » Risk analysis reports prioritizes risk severity
- » Reports include remediation tips based on CVE information

### Report Formats

- » HTML, PDF, CSV Reports

### Assessment Event Notification and Integration

- » Syslog
- » Email
- » Incident management ticketing integration
- » Real-time dashboard

## DAS Virtual Appliance - System Requirements

	Host	DAS VM Configuration
Processor	Pentium Dual Core	1 CPU
Memory	3GB and up	2GB
Hard Drive	Minimum of 10GB available disk space up-to 50GB	50 GB
Network	LAN Network connection	
Operating System	Any operating system supported by VMWare	



### 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-DAS\_0110rev1