

SecureSphere Discovery and Assessment Server (DAS) Vulnerability Assessment and Configuration Audit

SecureSphere Discovery and Assessment Server (DAS) identifies database vulnerabilities and measures compliance with industry standards and best practices. Combined with sensitive data discovery and data classification, organizations can accurately scope security and compliance projects and prioritize risk mitigation efforts.

Vulnerability Assessment: Detect Exposed Databases

SecureSphere DAS provides a comprehensive list of over 1000 tests and assessment policies for scanning platform, software, and configuration vulnerabilities. The vulnerability assessment process, which can be fully customized, uses industry best practices such as DISA STIG and CIS benchmarks. It results in a set of detailed reports documenting vulnerabilities that put databases at risk, as well as configurations that deviate from defined standards.

Discovery and Classification: Locate Sensitive Data

SecureSphere DAS identifies where databases are located on the network and surfaces “rogue” databases. SecureSphere scans the databases for sensitive data that is the focus of security and compliance projects. The results highlight well-known and custom sensitive data types, and track their location down to the database object, row and column. Object and column level classification enables organizations to focus on data in scope for security and compliance projects and configure granular policies to reduce the resource impact of these projects.

Virtual Patching: Protect Before Patches Are Available

SecureSphere DAS enables protection against attempts to exploit vulnerabilities when deployed with SecureSphere Database Firewall (DBF). Customers can set real-time security policies to block or alert on attempts to exploit vulnerabilities. This allows for immediate protection while patches are developed by the software vendors, thoroughly tested and safely deployed on the database servers.

User Rights Management: Find Excessive Rights

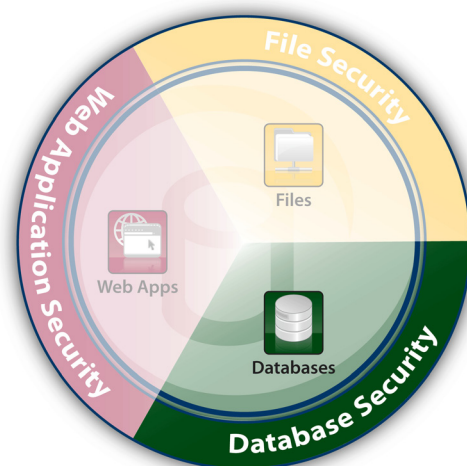
SecureSphere DAS enables automatic aggregation and review of user rights with the User Rights Management for databases (URMD) add-on option. URMD supports a focused analysis of rights to sensitive data and the identification of excessive rights and dormant accounts based on organizational context, object sensitivity and actual usage. Using URMD organizations can demonstrate compliance with regulations such as SOX, PCI 7, and PCI 8.5 and reduce the risk of a data breach.

Database Auditing and Protection: the Next Step for Data Security

For complete visibility and control of user access to sensitive data, SecureSphere DAS can be extended to include database activity auditing (DAM). Combining SecureSphere DAS and DAM enables administrators to define and deploy granular, focused audit policies making this powerful solution more effective and easier to use.

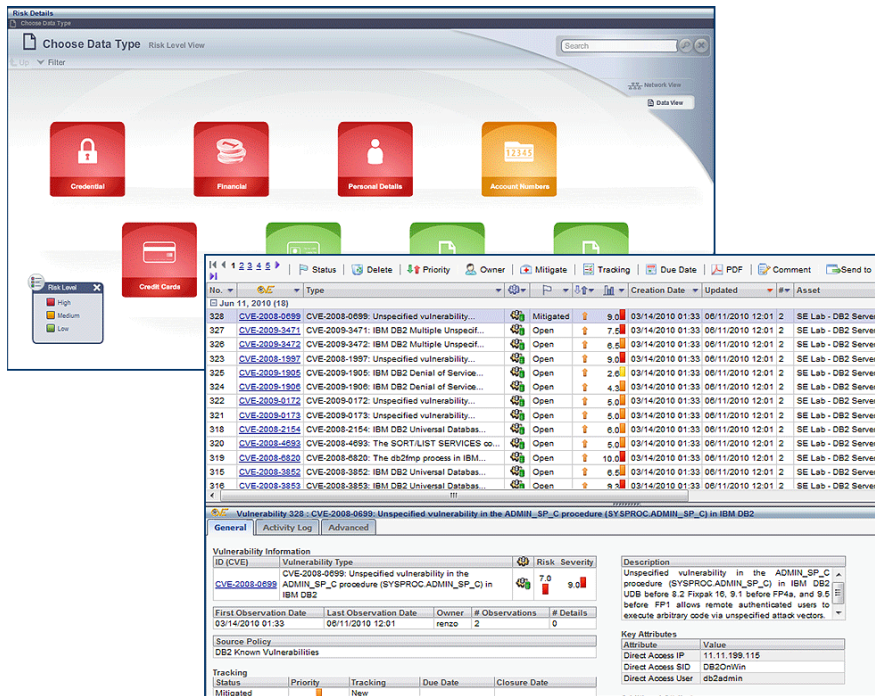
Discovery and Assessment Server Benefits

- » Detect database vulnerabilities based on the latest research by Imperva ADC
- » Audit configurations and measure compliance with industry standards and best practices
- » Identify databases that contain sensitive data, surface “rogue” databases
- » Virtually Patch vulnerabilities via integration with SecureSphere Database Firewall (DBF)
- » Calculate the risk to data based on data sensitivity and the severity of vulnerabilities



Data Risk Analysis: Putting it All Together

SecureSphere DAS enables educated decision making by providing a combined analysis of vulnerabilities and affected sensitive data. SecureSphere calculates the risk associated with each data asset based on data sensitivity and the severity of platform and database vulnerabilities. A graphical dashboard with drill down capabilities supports risk-focused prioritization of risk reduction efforts.



SecureSphere Discovery and Assessment Server

Understand areas of risk using the graphical risk explorer, track and mitigate vulnerabilities from the management console

About Imperva

Imperva is the global leader in data security

Thousands of the world's leading businesses, government organizations, and service providers rely on Imperva solutions to prevent data breaches, meet compliance mandates, and manage data risk. Underscoring Imperva's commitment to data security excellence, the Imperva Application Defense Center (ADC) is a world-class security research organization that maintains SecureSphere's cutting edge protection against evolving threats.

Imperva
Headquarters
3400 Bridge Parkway, Suite 200
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-0810rev1

