IMPERVA®

SecureSphere Database Assessment

Vulnerability Assessment and Configuration Audit

Database Assessment 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

SecureSphere Database Assessment 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 Database Assessment provides a comprehensive list of over 1500 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 Database Assessment 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 Database Assessment 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

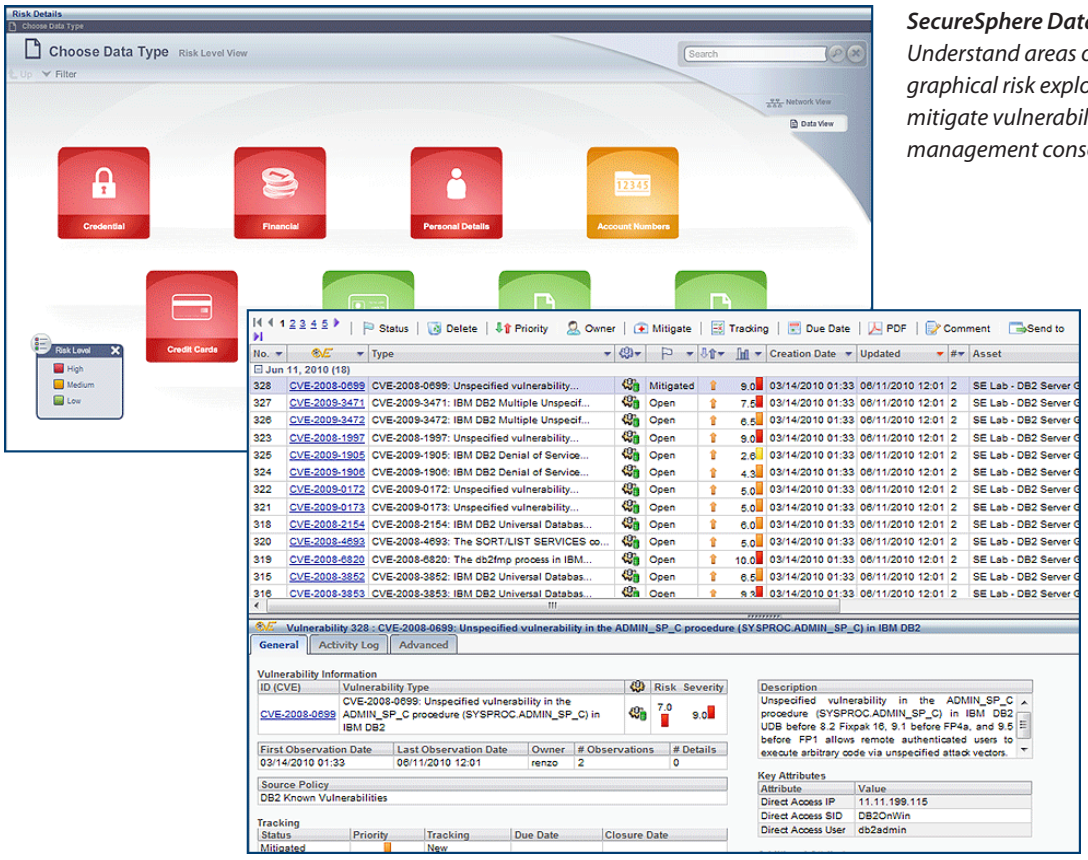
SecureSphere Database Assessment enables automatic aggregation and review of user rights with the User Rights Management for databases (URMD) add-on option. URMD supports a focused analysis of rights to sensitive data and the identification of excessive rights and dormant accounts based on organizational 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 Database Assessment can be extended to include database activity auditing (DAM). Combining SecureSphere Database Assessment and DAM enables administrators to define and deploy granular, focused audit policies making this powerful solution more effective and easier to use.

Data Risk Analysis: Putting it All Together

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

About Imperva

Imperva, pioneering the third pillar of enterprise security, fills the gaps in endpoint and network security by directly protecting high-value applications and data assets in physical and virtual data centers. With an integrated security platform built specifically for modern threats, Imperva data center security provides the visibility and control needed to neutralize attack, theft, and fraud from inside and outside the organization, mitigate risk, and streamline compliance.

IMPERVA®

www.imperva.com