

Sensitive Data Discovery

The need for enterprises to take effective measures to protect their sensitive data has never been greater. With data breaches leading the news, regulators and legislators are imposing higher standards for protecting sensitive data, and increasing penalties for offenders.

Understanding where to prioritize database security and compliance efforts is not a simple task. How can an enterprise tell the difference between databases containing sensitive information and those containing insignificant information? The answer is sensitive data discovery.

DbProtect's Sensitive Data Discovery capability locates and identifies sensitive data stored in databases across the enterprise. It discovers where sensitive data resides, including test and non-production environments, categorizes data according to confidentiality and business impact, and generates audit-ready reports. This qualification of sensitive data allows an organization to prioritize vulnerability assessment efforts and review user rights and access entitlements to Personally Identifiable Information (PII), and other sensitive assets. The process allows organizations to implement appropriate access controls and eliminate and enforce unnecessary access to sensitive data. Sensitive Data Discovery and the Database Discovery features of DbProtect's Vulnerability Management allow organizations to isolate and protect the sensitive data critical to their success.

5 Key Steps to Ensuring Database Security

In order to effectively secure their databases, organizations must address five critical requirements:

- 1. Isolate Sensitive Databases:** Maintain an accurate inventory of all databases deployed across the enterprise and identify all sensitive data residing on those databases.
- 2. Eliminate Vulnerabilities:** Continually assess, identify and remediate vulnerabilities that expose the database.
- 3. Enforce Least Privileges:** Identify user entitlements and enforce user access controls and privileges to limit access to only the minimum data required for employees to do their jobs.
- 4. Monitor for Deviations:** Implement appropriate policies and monitor any vulnerabilities that cannot be remediated for any and all activity that deviates from authorized activity.
- 5. Respond to Suspicious Behavior:** Alert and respond to any abnormal or suspicious behavior in real-time to minimize risk of attack.



DbProtect's Complete Enterprise Solution

COLLECT

DbProtect collects data detailing an organization's database ecosystem through an automated discovery process.

ANALYZE

DbProtect analyzes the data to highlight areas where risks and vulnerabilities reside and where database security process improvements are needed.

REMEDiate

Based on this analysis, DbProtect provides tools and detailed remediation instructions to eliminate database vulnerabilities.

ENFORCE

DbProtect enforces database security processes by monitoring and responding to deviations from authorized behavior.

Types of Sensitive Data include:

- Taxpayer IDs
- Employee names and addresses
- Dependent information
- Credit card numbers
- Intellectual property
- Classified information

Sensitive data discovery and protection is a key requirement in regulatory mandates such as PCI DSS, NIST 800.53, HIPAA, DISA STIG and others.

Effective database security and compliance requires organizations to ask the following questions:

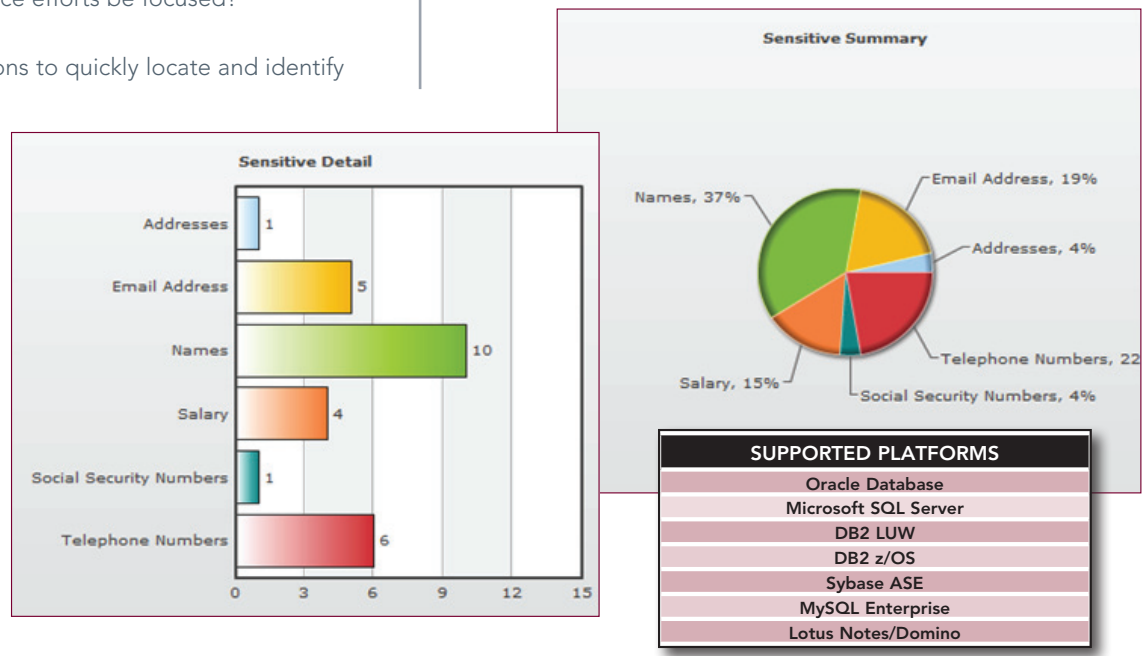
- What are the high value databases that require protection?
- Which databases contain social security numbers?
- What columns contain credit card information?
- Where should compliance efforts be focused?

DbProtect allows organizations to quickly locate and identify sensitive data stored in databases, generate effective database security policies, and prioritize database vulnerabilities. This facilitates rapid remediation of the vulnerabilities that pose the highest threat, and allows organizations to meet or exceed the mandatory requirements of compliance regulations.

SUMMARY

DbProtect’s Sensitive Data Discovery:

- Provides pre-defined templates for PCI, HIPAA and PII searches
- Discovers where all sensitive data resides, including test and non-production environments
- Quickly categorizes discovered data according to confidentiality impact
- Generates audit-ready reports detailing when repositories were searched and what sensitive information they contained
- Prioritizes vulnerability assessment efforts
- Review user rights to PII databases to enforce restricted access
- Provides easy-to-use reports
- Allows custom search capabilities for locating enterprise or industry-specific sensitive data types



ABOUT APPLICATION SECURITY, INC. (APPSECINC)

AppSecInc is a pioneer and leading provider of database security and compliance solutions for the enterprise. By providing strategic and scalable software-only solutions – AppDetectivePro for auditors and IT advisors, and DbProtect for the enterprise – AppSecInc supports the database lifecycle for some of the most complex and demanding environments in the world across more than 1,300 active commercial and government customers.

Leveraging the world’s most comprehensive database security knowledgebase from the company’s renowned team of threat researchers, TeamSHATTER, AppSecInc products help customers achieve unprecedented levels of data security while reducing overall risk and helping to ensure continuous regulatory and industry compliance.

For more information, please visit: www.appsecinc.com | www.teamshatter.com

For a free database vulnerability assessment visit: www.appsecinc.com/downloads/appdetectivepro

Follow us on Twitter: www.twitter.com/appsecinc | www.twitter.com/teamshatter

APPLICATION SECURITY, INC.®
www.appsecinc.com