

Achieving Successful Database Risk Analysis

Today's enterprise organization encounters an infinite number of risks across all aspects of its business. It has become imperative to map IT risks to business objectives relative to database vulnerabilities and misconfigurations. Understanding where to prioritize remediation efforts in the database is challenging for large organizations that rely on thousands of databases to house sensitive information.

DbProtect's Risk Analysis enhances the value of DbProtect's Precision Database Activity Monitoring solution by prioritizing database vulnerability remediation processes and focusing resources. Risk Analysis identifies risk scores by levels of exploitability, susceptibility and business impact for each vulnerability identified by DbProtect Vulnerability Management. From the risk analysis, organizations can enact focused, timely, and properly prioritized remediation efforts.

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.

PRIORITIZED RISK CONCENTRATION

- Categorize database risks
- Identify the most immediate and threatening set of risks for quick response
- Allows quick response
- Prioritize resource allocate
- Improve overall risk mitigation process with materiality intelligence

PRIORITIZING RISKS WITH THE GREATEST MATERIAL THREAT

Map database risk through prioritized rankings back to the potential business impact. Establish a baseline for quantifying vulnerability remediation through visualized analytics.

Answer questions such as:

- Which high value databases require immediate remediation?
- How do I collect and normalize existing data from at-risk databases?
- How to document where all database risks are coming from?
- Can large data sets be managed for insight across data, impact and asset role?
- Can the business impact of a database vulnerability against its business materiality be weighed?

Analytics of Single Database Risk

THE DATABASE SECURITY, RISK AND COMPLIANCE LIFECYCLE

Understanding business risks across the database environment is a critical step. DbProtect’s Risk Analysis enables enterprises to create custom reports through advanced visualization and dashboard capabilities to effectively assess and measure risk for continuous database security process control and compliance.

- Improve overall risk mitigation process
- Quickly categorize discovered data according to materiality impact
- Identify, prioritize and measure the database risks that are most threatening enterprise-wide
- Generate audit-ready reports detailing which vulnerabilities found and how they are weighted against exploitability, susceptibility and potential impact
- Prioritize vulnerability remediation efforts
- Isolate and measure each risk at a granular level

RISK FEATURES

- Enterprise ready to report across multiple heterogeneous databases and file systems for potential database vulnerabilities
- Normalized scoring and business classification
- Ability to determine which database vulnerabilities represent the highest risk score relative to its business impact
- Customizable views and dashboard capabilities with advanced analytics
- Maximum extensibility to extend outward from DbProtect to other data sources
- Enterprise class software; no network hardware required

Risk	High
Check Performed	Permission on registry extended proc
Description	Permission to execute the registry extended stored procedures have been granted to a user or group.
Version Affected	All versions of Microsoft SQL Server
CVE Identifier	CVE-NO-MATCH
CCE Identifier	CCE-NO-MATCH
Summary	Microsoft SQL Server provides a set of extended stored procedures which allow database users to read and write from the registry. If not configured properly, the registry extended stored procedures can be used to read or write sensitive information from the registry.
Overview	The registry extended stored procedures allow Microsoft SQL Server to read, write, and enumerate values and keys in the registry. They are used by Enterprise Manager to configure the server. These procedures should be closely guarded because of the sensitive information stored in the registry. Typical information found in the registry includes password hashes as well as clear text password. The sensitivity of these procedures are exacerbated if Microsoft SQL Server is run under the Windows account Local System. Local System can read and write nearly all values in the registry, even those not accessible by the administrator. The list of registry extended stored procedures include xp_regaddmultistringxp_regdeletekeyxp_regdeletevaluexp_regenumvaluesxp_regenumkeysxp_regreadxp_regremovemultistringxp_regwritexp_instance_regaddmultistring xp_instance_regdeletekey xp_instance_regdeletevalue xp_instance_regenumkeys xp_instance_regenumvalues xp_instance_regread xp_instance_regremovemultistring xp_instance_regwriteIf the MSSQLServer service runs under the LocalSystem account, this call will allow a database user to read a password hash out of the registry. The following example demonstrates how this is accomplishedEXEC xp_regread 'HKEY_LOCAL_MACHINE', 'SECURITY\SAM\Domains\Account', 'F'Unlike the xp_cmdshell extended stored procedure, which runs under a separate context if executed from a non-Sysadmin login, the registry extended stored procedures always execute under the security context of the MSSQLServer service. By default, the public group has permission to execute xp_regread. All other registry extended stored procedures default to only being executable by the dbo in the master database (typically Sysadmins only). In SQL Server 2000 Service Pack 4 (SP4) and above, two REG_MULTI_SZ registry keys - 'Xp_regread Allowed Paths' and 'Xp_regwrite Allowed Paths' can be used to control the paths that can be accessed by these extended procedures. Only the users granted the system administrator server role now have unrestricted access to all the paths; others are limited to the registry paths specified in the keys mentioned above. For default instance of SQL Server 2000 the keys can be found under: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer\MSSQLServer\ExtendedProceduresFor a named instance of SQL Server 2000 the keys can be found under HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer\MSSQLServer\ExtendedProcedureFor a default and a named instance of SQL Server 2005 and 2008 the keys can be found under HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server\MSSQLServer\ExtendedProcedureIn SQL Server 2005 and 2008, the keys are absent by default, but can be manually added to limit or allow access to certain registry paths. When the keys are not present, the access is limited to the registry paths that contain entries relevant to the concerned instance. WARNING!!! If you remove public permissions, some features of third-party applications -- or even built-in features of Microsoft SQL Server -- may break. While this level of security is desirable, it's often inappropriate. In most scenarios, AppSecInc does not recommend disabling public permissions from system objects without thoroughly testing your application.
Fix	You should revoke permissions to execute any of the registry extended stored procedures from any users. By default, members of the sysadmin server role are able to execute any of the registry extended stored procedures because they are mapped to dbo. Run the following command to revoke extraneous grants on the registry extended stored procedures.REVOKE EXECUTE ON xp_regread FROM [user or group]If you determine that an attacker has accessed the SAM database, you should reset any passwords for all users on the system.

SUMMARY

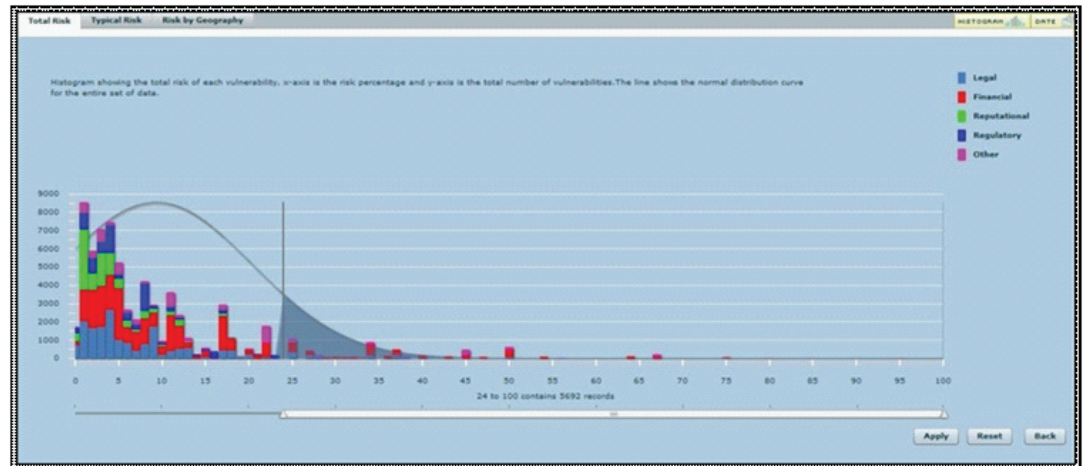
DbProtect’s Risk Analysis enhances DbProtect’s Precision Database Activity Monitoring solution by helping organizations to:

- Categorize database risks
- Identify the most immediate and threatening set of risks for quick response
- Enable quick response
- Prioritize resource allocations
- Improve the overall remediation process with material intelligence



Risk Assessed by Specific Date Range

Risk Materiality - Finding the 'critical few'



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