

MANAGE SQL SERVER SECURITY AND PERMISSIONS

SQL secure™

SOLUTIONS FOR SECURITY & COMPLIANCE

Idera SQL secure is a security analysis solution that identifies SQL Server security violations and ensures security policies are enforced. Find out who has access to what and identify each user's effective rights across all SQL Server objects. Alert on violations of your corporate policies, monitor changes made to security settings, and provide security audit reports as well as recommendations on how to improve your security model.

PRODUCT HIGHLIGHTS

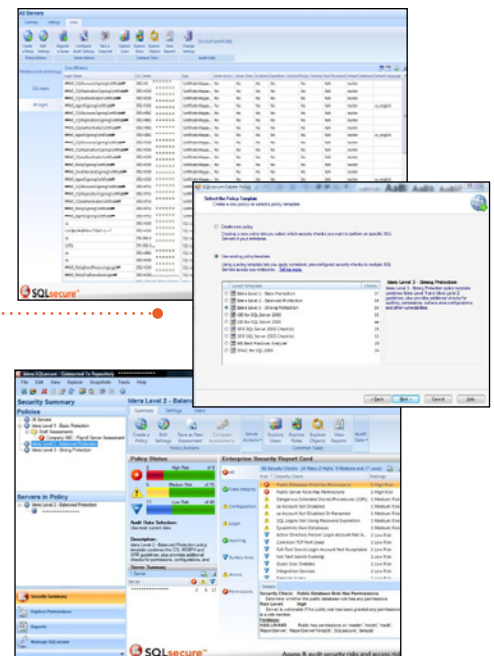
- Identify vulnerabilities and harden security across your SQL Servers
- Diagnose and protect against violations of your security policies and security best practices
- Analyze and manage user permissions across all SQL Server objects with our powerful security model analysis
- Create policies using customizable templates for various security level needs

Enterprise View of All Users Flexible grid lets you analyze and export all the SQL Server logins in your enterprise.

SQL secure can import and deploy policy templates with recommendations from authorities such as DISA SRR, CIS, SNAC, and more. This will assist in compliance with guidelines such as PCI DSS and SOX.

SQL secure Security Report Card rates your SQL Servers against the security risks and compliance issues. Drill down for more details and recommendations.

"SQL secure is an essential tool in preparing for an audit. The ability to link in to Active Directory and see all the effective permissions for any given group is indispensable. Also, alerts from SQL secure keep me on top of things at all times. With SQL secure, we are more confident that our databases are secure and that we can meet audit requirements." - SENIOR SQL DBA, MAJOR U.S. FINANCIAL SERVICES FIRM



WHY SQL secure?

Because of the many different and complex ways to grant access to SQL Server databases – including server and database roles, Active Directory and local groups, inherited permissions, explicit grants and denies, just to name a few – it is virtually impossible to manually analyze a security model across instances or determine a user's rights on specific database objects. SQLsecure does this for you, answering the important question "Who can do what, where, and how on my SQL Servers?" SQL secure provides a comprehensive, automated solution for analyzing, monitoring, and reporting on security access rights in SQL Server databases.

DOWNLOAD A FREE EVALUATION TODAY AT WWW.IDERA.COM

KEY BENEFITS

Powerful Security Model Analyses: gather a complete picture of the security of your SQL Server environment with the analysis and reporting tools provided by SQLsecure.

Analyses available include:

- **Effective User Permissions** – select a user and discover all assigned and effective rights and permissions at the server, database and object level.
- **Users and Groups** – drill up or down on users and groups. From a group, see the list of group members and select a member for further analysis. From a user, see the group memberships and drill upwards to review the inherited permissions.
- **Object Access Rights** – browse and analyze the full SQL Server object tree from server level down to object level, tables, roles, endpoints and more. Instantly view assigned and effective/inherited permissions and security related properties at any object level.

Continuous Change Monitoring – provides the ability to capture snapshots of the security model on a regularly scheduled or ad-hoc basis in order to identify changes to access rights and security settings. This enables rapid analysis and detection of unwanted changes to security settings.

Comprehensive Security and Entitlement Reporting – use the report catalog to track vulnerabilities, security changes and user entitlement over time.

TECHNICAL FEATURES

SECURITY ANALYSIS & REPORTING

- **Pre-defined Policy Templates:** Combines the most well known industry standards into 3 distinct levels, (Basic-Balanced-Strong) that define realistic guidelines for protecting SQL Server from the most common intrusion attacks
- **Effective Rights Analysis:** analysis of users' effective rights shows you how and where each right is granted, making it easy to pinpoint exactly what changes need to be made in order to close security holes.
- **SQL Server Files, Directories, and Registry Settings:** browse and analyze all files, directories and registry settings associated with SQL Server and determine ownership as well as explicit and inherited security rights
- **SQL Server Surface Area and Protocols:** identifies services, ports, protocols and API's that may allow SQL Server to be attacked by a malicious user. Enables you to understand and standardize which services you really need started or activated in your environment in order to reduce risk
- **OS Security Analysis:** assess the OS setup to identify issues that would compromise SQL Server security.
- **Powerful User Analysis:** analyze membership to powerful server roles and groups such as administrators, system administrators and security administrators so you can ensure this level of access is warranted.
- **Security Scorecard:** lists potential security concerns on your SQL Servers such as cross database chaining and gives you the ability to drill down to view the full details.
- **Detection of Unresolved Windows accounts:** SQLsecure shows you all logins on the target server, as well as any unresolved Windows accounts or groups.
- **Server Security Properties:** show all security related properties for servers including: version and patch level, authentication mode, audit mode, proxy account, and cross database chaining.
- **Comprehensive Security Model Version History and Baselining:** the SQLsecure Repository keeps a complete history of SQL Server security settings, providing the ability to designate a baseline to compare against future snapshots to detect changes. This also provides a valuable audit trail for forensic analysis.
- **Powerful Reporting:** use built-in standard reports for security auditing and compliance; plus, produce custom reports or perform custom analysis via the data stored on the SQLsecure repository. Data can also be exported to Excel.
- **Cross-server Reporting:** provides the ability to show security state from a global view (e.g. all instances with guest accounts enabled).

ENTERPRISE MANAGEMENT FEATURES

- **Central Console for Analysis and Auditing:** provides an easy-to-use single point of control to manage the creation of collection rules, view collection history, analyze user access rights and more.
- **Configurable Data Collection:** define exactly what SQL Server security information you want to gather and when. Gathers from SQL Server, OS, File System, Registry and AD.
- **Central Repository of Security Information:** all data collected by SQLsecure is stored in a central repository for easy reporting and forensic analysis.

REGULATIONS SUPPORTED

SOA Sarbanes-Oxley Act Section 404 (COSO, CobiT)
VISA CISP
HIPAA Health Insurance Portability And Accountability Act of 1996
GLBA Gramm-Leach-Bliley Act of 1999
NERC Standard 1200
FISMA (NIST 800-53 Draft)
Basel II Capital Accord (ISO 17799:2000)
PCI DSS v 1.1 Payment Card Industry

STANDARDS, POLICIES & GUIDELINES SUPPORTED

ISO 17799:2000
* CIS Benchmark for SQL Server
* DISA Database STIG Security Checklist for MS SQL Server
* NSA Systems and Network Attack Center (SNAC) Guidelines for SQL Server 2000
* *contains related policy templates*

SYSTEM REQUIREMENTS

MANAGEMENT CONSOLE

- Windows 2000 Server SP4 or later, Windows XP SP2 or later, Windows Server 2003 SP2 or later, Windows Server 2008, Windows Server 2008 R2, Windows Vista Business and Enterprise, Windows 7
- Microsoft .NET 2.0 SP1 or later
- IE 7.0 or later for online Help
- MDAC 2.8 or later

DATA REPOSITORY

- SQL Server 2005 SP1 or later, SQL Server 2008, SQL Server 2008 R2

MICROSOFT SQL SERVER FOR AUDITED INSTANCES

- SQL Server 2000, SQL Server 2005 or later, SQL Server 2008, SQL Server 2008 R2

SQLsecure does not install any components, DLLs, scripts, stored procedures or tables on the SQL Server instances being monitored.

Idera | BBS Technologies

802 Lovett Blvd Houston, Texas 77006

PHONE 713.523.4433 | TOLL FREE 877.GO.IDERA (464.3372)

FAX 713.862.5210 | WEB www.idera.com

