SQL Secure

MANAGE SQL SERVER SECURITY & PERMISSIONS

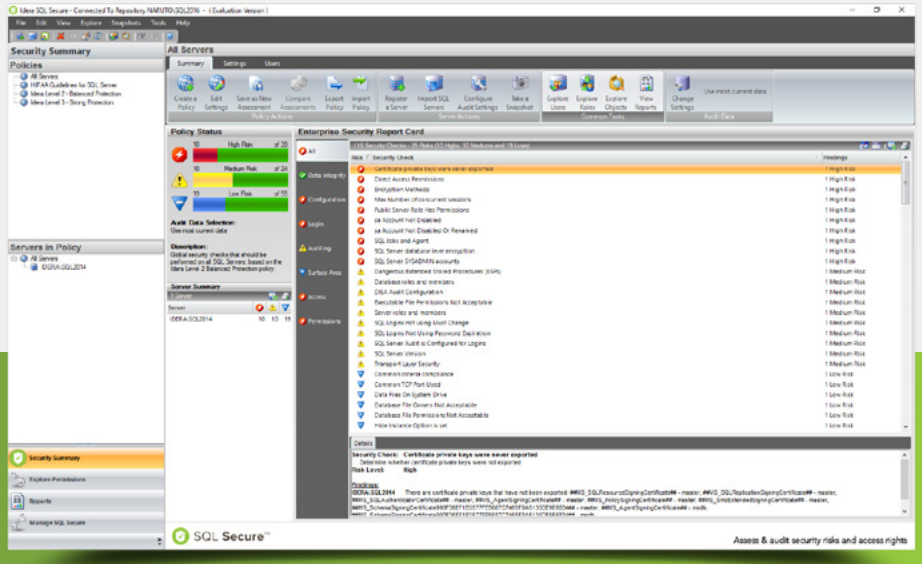
IDERA SQL Secure discovers security vulnerabilities and user permissions for SQL Server instances deployed on physical, cloud, and virtual hosts. Find out who has access to what and identify each user's effective rights across all SQL Server and Azure SQL Database objects. Alert on violations of your corporate policies, monitor changes made to security settings, and generate security audit reports as well as recommendations on how to improve your security model.

WHY SQL SECURE?

Because of the many different and complex ways to grant access to SQL Server whether they are on premises or in the cloud (Amazon or Azure) - 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. SQL Secure does this for you, answering the important question, "Who can do what, where, and how on my SQL databases?" Hybrid environments that combine on premises and in-cloud deployments are becoming more common as organizations strive to incorporate new technologies into their deployments. SQL Secure provides a comprehensive, automated solution for analyzing, monitoring and reporting on security access rights for SQL Servers (on premises, private cloud, Amazon EC2 or Azure VM), Amazon RDS for SQL Server, and Azure SQL databases.

PRODUCT HIGHLIGHTS

- Identify vulnerabilities in SQL Server and Azure environments
- Harden security policies across SQL Server and Azure databases
- Rank security levels with the security report card
- Analyze and report on user permissions across database objects
- Comply with audits using customizable regulatory guideline templates



Start for FREE!

KEY BENEFITS

Powerful Security Model Analyses Gather a complete picture of the security of your SQL Server, Amazon RDS for SQL Server, and Azure SQL databases, whether deployed on physical, virtual, or cloud hosts, with the in-depth analysis and reporting tools provided by SQL Secure. Assess the effectiveness of user permissions, view details about users and group, and browse object access rights with an intuitive user interface.

Regulatory Policy Templates Use the IDERA and industry standard policy templates to harden your SQL Server security model. By creating policies from these templates for regulatory compliance, you can enforce consistent security settings across your enterprise and proactively assess when and where vulnerabilities exist. Choose from templates for CIS, DISA STIG, GDPR, HIPAA, NERC, NIST, PCI DSS, and SOX.

Continuous Change Monitoring SQL Secure 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.

Entitlement Reporting Use the report catalog to track vulnerabilities, security changes, and user entitlement over time, with built-in report formats or customized reports using Microsoft Reporting Services.

Comprehensive Security Additional security audit rules and security checks give greater visibility for database access checks, configuration checks, data encryption checks, and permission checks for on premises, hybrid, and in-cloud environments.

TECHNICAL FEATURES

Security Analysis

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.

Database Roles Permissions View SQL Server, Amazon RDS for SQL Server, and Azure SQL database role members and sub-roles assigned and their effective permissions.

Weak Password Detection Analyzes password health of SQL Server logins and reports on when passwords are weak or blank which would cause a susceptible to intrusion situation.

Surface Area and Protocols Identifies services, ports, protocols and APIs that may allow SQL Server, Amazon RDS for SQL Server, or Azure SQL databases 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.

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.

Detection of Unresolved Windows Accounts View 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.

Self-auditing Monitor all activity related to SQL Secure administration.

Security 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.

Reporting Services Shows details of services such as log-on and configuration.

Security Scorecard Lists potential security concerns on your SQL Servers such as cross-database chaining and drill down to view the full details of the diagrammed relationships.

History and Baselining The SQL Secure 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 and compliance reports.

Powerful Reporting Built-in standard reports provide detailed information for security auditing and compliance purposes. Produce custom reports or perform custom analysis via the data stored on the SQL Secure repository. Data can also be exported to Excel.

Risk Assessment Security audit rules provide visibility for database access checks, configuration checks and permission checks.

Security Checks Additional checks for data protection, encryption, and firewall rules for the SQL Server, Amazon RDS for SQL Server, and Azure SQL database platforms increase security audit coverage.

Cross-server Reporting Shows security state from a global view (e.g. all instances with guest accounts enabled).

Enterprise Management

Central Console for Analysis & 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.

Integrated Cloud Support For DBaaS: Azure-hosted and Amazon-hosted SQL Server databases, including Azure SQL Database and Amazon RDS for SQL Server. For IaaS: SQL Server running on Azure Virtual Machines (VMs) and Amazon EC2

Cloud Connectivity Connect to fully qualified domain names (instead of static IP addresses) for Azure VMs, Azure SQL Database instances, Amazon RDS and Amazon EC2 as registered servers.

Flexible Views Use the flexible grid view to audit and analyze user permissions. Sort, group, or export all SQL Server logins in your enterprise. View all users' assigned and effective rights and permissions at the server, database and object level.

Central Repository of Security Information All data collected by SQL Secure is stored in a central repository for easy reporting and forensic analysis.

Configurable Data Collection Define exactly what SQL Server security information you want to gather and when. Gathers from SQL Server on physical, virtual, or cloud hosts, Azure SQL Database, Amazon RDS for SQL Server, OS, File System, Registry, Active Directory (AD), Azure AD, and Amazon AD.

Automated Server Registration CSV import process provides improved support for large SQL Server environments with significant gains in time to value.

Server Group Tagging Enables DBA teams to assign servers to groups, then view and manage security policies according to group designations.