SQL Security Suite

POWERFUL TOOLS TO AUDIT AND SECURE SQL SERVERS AND DATA

Data security and regulatory compliance requirements have become increasingly evolving and complex. Data compliance is now considered a “Must-Have” and DBAs are tasked with the monumental job of providing an accurate audit trail of server activities such as database access, update actions, schema changes and security policy changes. They must also manage who can do what, where and how to the data by maintaining user roles and permissions and reporting on these access rights to others in the organization. IT auditors, on the other hand, must demonstrate compliance with regulatory and data security requirements with an audit trail of reports. Unfortunately, auditing, managing and reporting this information can often require countless hours or even custom development work.

To solve this challenge, IDERA has assembled vital technology together to address DBAs and IT Auditors critical needs. The SQL Security Suite contains full licenses to IDERA SQL Compliance Manager and SQL Secure with the first year of standard technical support included. Plus, when you buy as a bundle, you can save up to 40% versus buying each product separately!

KEY FEATURES AND USE CASES

Continuous, Flexible Auditing
Real-time monitoring and auditing of all data access, updates, data structure modifications and changes to security permissions. The type and detail of audit data collected is highly configurable and may be defined at the server, database and object level.

Notification of Suspect Activity
Receive immediate alerts on suspect server activity via e-mail or the event log. The alerting engine includes flexible alert definitions, alert templates, custom messaging, and alert reporting. Plus, alerts can be applied across the board, or to specific servers, databases, or tables, for more fine-grained control.

Sensitive Data Auditing
Audit any combination of columns and track who has issued “SELECT” statements against any table, whether they are end-users or privileged users. Audit the most sensitive data contained in your databases, right down to the column level. Determine where sensitive data resides whether in individual columns or a sensitive data set that spans across multiple tables, and add to the audit monitor.

Compliance to Regulatory Requirements
Use pre-built policy templates to harden your SQL Server security model. By creating policies from these templates for PCI, SOX, HIPAA, DISA STIG, FERPA, CIS and NERC compliance, you can enforce consistent security settings across the enterprise and proactively assess when and where vulnerabilities exist.

Powerful Reporting and Analytics
A variety of ‘out of the box’ reports, developed in conjunction with industry experts Ernst and Young and Information Shield Inc., address a broad range of auditing and security reporting needs and demonstrate compliance to multiple industry regulations. Track vulnerabilities, security changes, and user entitlement over time with built-in report formats or customize reports using Microsoft Reporting Services.

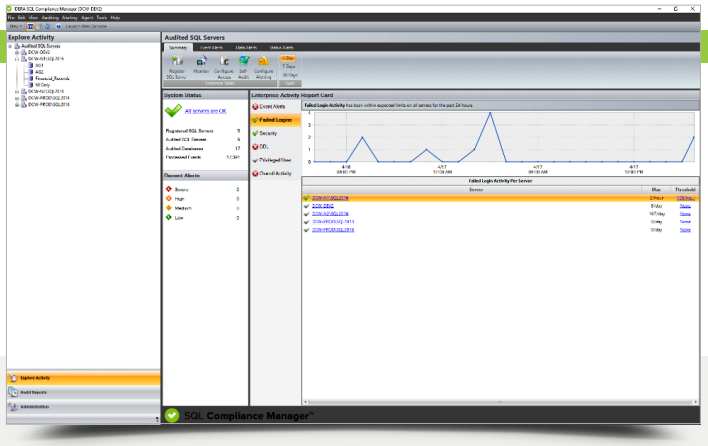
Weak Password Detection
Analyze password health of SQL Server logins and report on when passwords are weak or blank which would cause a susceptible to intrusion situation.

Continuous Change Monitoring
Capture snapshots of the security model on a regularly scheduled or ad-hoc basis to identify changes to access rights and security settings. This enables rapid analysis and detection of unwanted changes to security settings to minimize risk. Plus, audit data changes on any table to compare before and after data values resulting from inserts, updates and deletions.

Security Model Analysis
Gather a complete picture of the security of SQL Server and Azure environments with the in-depth analysis and reporting tools. Assess the effectiveness of user permissions, view details about users and groups, and browse object access rights. Plus the user-friendly schema of the audit data repository enables rapid development of ad-hoc queries and reports for detailed forensic analysis.

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 cloud environments.

Start for FREE!



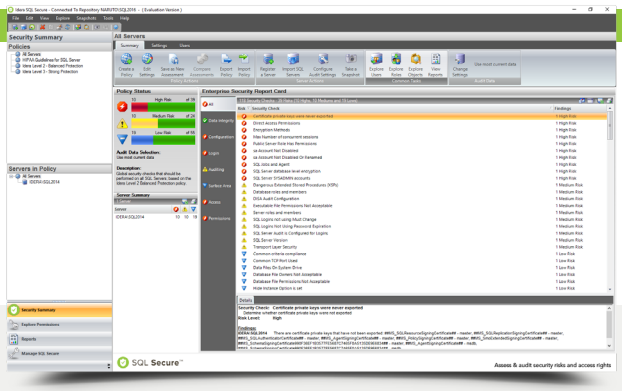
SQL Compliance Manager

MONITOR, AUDIT AND ALERT ON SERVER ACTIVITY AND CHANGES

- Audit sensitive data and see who did what, when, where, and how
- Monitor and alert on suspicious activity to detect and track problems
- Pre-built templates for PCI, HIPAA, FERPA, SOX, CIS, DISA STIG and NERC
- Select from over 25 pre-defined compliance reports and create custom views
- Minimize server impact with a lightweight data collection agent
- Access via desktop console or web console and remotely execute actions

"**SQL Compliance Manager** has the ability to audit virtually every activity occurring inside SQL Server. This, combined with the built-in reports and ad-hoc reports you can create yourself, allows you to identify and report on any SQL Server activity you want."

- SQL Server Performance.com



SQL Secure

MANAGE SQL SERVER & AZURE SQL SECURITY AND PERMISSIONS

- Identify existing vulnerabilities in your SQL Server and Azure environments
- Harden security policies across SQL Server & Azure SQL databases
- Rank security levels with the security report card
- Analyze and report user permissions across database objects
- Comply with audits using customizable templates for PCI, HIPAA and more

"**SQL Secure** automates user permission analysis — a job that can be very time-consuming. It tells me at a glance what access a particular user has. Via filters and audits, I can easily keep track of changes to objects, permissions, logins, and group members."

- **Database Analyst**, Bass Pro Shops