idera™
TOOLS FOR SQL SERVER™

10 steps
TO SECURE YOUR SQL SERVER

In increasing numbers, information security professionals everywhere are realizing that when it comes to protecting your company's valuable assets, it's all about the data. News stories are released almost every day detailing data security breaches at organizations of all types. These breaches can be very expensive due to the cost to notify impacted customers or employees, and damaged company reputation. Those responsible for the breach often face disciplinary measures, up to and including termination.

In most organizations today, business critical and confidential data resides in some type of database, increasingly, SQL Server. As a result, SQL Server database security and compliance have become critical issues that must be effectively addressed to ensure an organization's overall security.

The goal is simple - minimize business risk, data theft, and data losses through good security practices. This whitepaper gives an overview of 10 key areas you need to focus on in order to ensure SQL Server security, and avoid finding your company in the headlines.

About Idera: Tools for SQL Server: Idera delivers a new generation of tools for managing the world's fastest growing database management system, Microsoft SQL Server. Idera's solutions help database administrators keep SQL Server running at optimum performance, ensure availability, speed recovery, ease compliance requirements, and dramatically reduce administrative overhead. Idera's products are amazingly simple to use, provide remarkable results, and can be installed in minutes. Idera is a Microsoft Gold Certified Partner with over 2,500 customers worldwide.

10 steps

TO SECURE YOUR SQL SERVER

step 1

KEEP SYSTEMS UP TO DATE ON SERVICE PACKS, PATCHES, AND NEW VERSIONS OF THE OS AND SQL SERVER.

Just like you need to change the oil in your car every 5,000 miles, you need to maintain your SQL Servers with the latest service packs and patches. Additionally, it's a good idea to plan ahead for upgrades to new versions of the OS and SQL Server in order to take advantage of the latest security advances.

If you are slow to install service packs and patches, or to upgrade to new versions of the OS and SQL Server, your servers will be more vulnerable to exploits. The cost to perform proactive maintenance is much cheaper than the cost to recover from a database security breach. Additionally, the longer you wait to upgrade to newer versions of SQL Server, the more difficult the upgrade becomes for your staff since they may not remember who wrote what custom code that needs to be migrated, why the data model is set up the way it is, etc.

Make sure you establish a standard, regularly scheduled process for rolling out service packs and patches. Additionally, start planning months ahead of time for upgrading to new versions of the OS and SQL Server so you can determine how to best take advantage of new security features.

Tools to help with this: Idera **SQLsecure** is a tool for assessing security across your SQL Servers. **SQLsecure** collects SQL Server version number and service pack as part of the overall security assessment it performs. The version number returned by **SQLsecure** will also reflect the latest patches applied, so you can determine which servers are out of date.

step 2

ENFORCE STANDARDS FOR SECURE PASSWORDS.

If you leave the keys in your car's ignition long enough, someone is going to steal your car. The same can be said for passwords. If you allow the use of non-existent or weak passwords on your SQL Servers, sooner or later, someone will find these accounts and take advantage of them.

10 steps

TO SECURE YOUR SQL SERVER

To ensure proper password security, you should:

- Ensure that passwords used by applications or services (especially SQL Server) are kept secret.
- In many cases, login names should also be kept confidential.
- Use the security options in SQL Server 2005 and Active Directory to enforce a policy requiring non-trivial passwords

Tools to help with this: If you are using SQL Server 2005, use the built-in security options to enforce password complexity standards. For previous versions of SQL Server, there are many publicly available scripts you can use to identify accounts with weak or non-existent passwords.

» step 3

SECURE THE FULL ENVIRONMENT, INCLUDING THE OS AND NETWORK

Just like your house would not be secure if you lock your doors, but leave the windows open, your SQL Server is not secure if the OS, Network or Applications connecting to the SQL Server have security vulnerabilities. Gaps in security in any of these three areas can lead to a SQL Server security breach, so it is a good idea to take additional actions to secure your full environment.

Remember things like:

- Keep SQL Server off the Internet.
- Limit physical access to the server.
- Limit the number of accounts with access to the server and change default account names and other settings (for example, disable the Windows guest account).
- Limit use of file shares and ensure they are secured properly.
- Be sure to use firewall and anti-virus protection.
- Secure the SQL Server registry, directories and files.
- Limit administrator group membership.
- Enforce secure coding practices and test applications for security gaps.
- Follow proper security practices when setting up middleware or report servers.

Tools to help with this: Microsoft has many documents and knowledge base articles that provide more detail and best practices on how to ensure server and application security.

10 steps TO SECURE YOUR SQL SERVER

step 4

ENSURE APPROPRIATE SQL SERVER SETUP

The more windows and doors your house has, the more things you have to worry about securing. The same goes for SQL Server – the more capabilities you enable on the server, the more potential vulnerabilities you have. With regard to security, less is more.

To minimize your security vulnerabilities, remember things like:

- Only run the services you need. For example, if you aren't using analysis services don't run them.
- Limit the communication protocols in use.
- Change the default port setting in environments that need to be highly secure.
- Disable features such as extended stored procedures (like xp_cmdshell and OLE automation).
- Don't use mixed authentication, if possible.
- Change net config settings to hide SQL Server from auto discovery.
- Remove all sample databases, accounts, or other code from the server.
- Limit Server Role memberships.
- Turn on error and security logging.

Tools to help with this: Idera **SQLsecure** checks most of these settings across your SQL Servers and reports back where you have potential security concerns.

step 5

REGULARLY ASSESS WHO CAN ACCESS YOUR SQL SERVERS AND TAKE ACTION TO LIMIT ACCESS.

Just like you maintain tight control over who has keys to your house, you also need to limit access to your SQL Servers to those who have a legitimate reason to have it. There are few audits that haven't turned up accounts with access to a SQL server that should not have been there. In fact, a major bank discovered during an audit that a consultants group nested 2 levels down under a domain group had system administrator access to a production database. There were 120 users in this group.

If people have access to your SQL Servers that shouldn't, they can make inappropriate use of that access. The risk comes not only from malicious users who might use the access to steal data, but also from inexperienced users who could inadvertently cause serious problems on your production databases.

10 steps

TO SECURE YOUR SQL SERVER

To thoroughly assess who has access to your SQL Servers, you should take the following steps: Get a list of all login accounts (users and groups) for each SQL Server. Include both Windows and SQL Server accounts in this list.

- Expand the groups to obtain a complete list of members.
- Delete the extra logins from SQL Server that should not have access.
- Delete the Windows users and/or groups that should not have access.
- Limit membership in powerful OS groups, like the Windows Admin user group, to the bare minimum needed for people to do their jobs.
- Do not permit OS defined groups, like the "Everyone" group, to have access to the SQL Server.

Tools to help with this: Idera **SQLsecure** can make this task a whole lot easier for you. **SQLsecure** automatically generates a complete list of all users with access to your SQL Server, across Windows, Active Directory, and SQL Server, including users that have access as a result of group membership.

» step 6

ASSESS WHAT ACTIONS USERS CAN PERFORM ON WHAT OBJECTS

Even if you provide your housekeeper with a key to your house, you would not also give her the combination to your safe. The same is true with your SQL Servers - just because someone needs access to one database or object on the server does not mean they should have access to everything. People that have privileges they shouldn't have may do things they shouldn't do. Don't tempt them.

As a result, it is critical that you regularly assess users' effective rights on the server and determine if those rights are appropriate to their business needs. Often users are granted more rights than they need due to human error, sloppy work (make a user sys admin and figure out the security later), or a misunderstanding of SQL Server security.

10 steps

TO SECURE YOUR SQL SERVER

To assess and limit user access, you should take the following steps:

- Delete the "Guest" user account from all databases, except the master and tempdb databases.
- Ensure all logins map to a valid user within a given database.
- Create database roles and use them.
- If you use fixed database roles, make sure you understand the permissions they grant (this is a frequent source of security mistakes).
- Use stored procedures and views for data access as opposed to defining access directly on tables.
- Encrypt column data that needs ultimate protection.
- Assess effective rights for all users who have access to the database. To determine effective rights you need to look at security assignments across all methods for assigning them - logins, groups, server and database roles, users mapping, grant, denies, schemas, etc. Since proper assessment can be very complex, tedious work, focus on your highly valuable data assets, like key tables containing confidential information.

Tools to help with this: Accurately assessing effective permissions on SQL Server objects is really, really, hard to do manually. Idera **SQLsecure** can perform this time consuming task for you. **SQLsecure** calculates both effective (derived) and assigned permissions for all users, on any database object, making it much easier to ensure that users have appropriate access rights.

» step 7

KEEP AN AUDIT TRAIL OF DATABASE ACTIVITY.

Just like you review your credit card statement each month to ensure all charges were legitimate, you should also audit database activity to keep a record of "who did what, when, where and how". Auditors or security officers will require that your organization monitor key database activities such as failed logins, escalation of privileges, schema changes and especially access to sensitive data. Once collected this information can serve many useful purposes:

- Help you detect suspect activity by type, volume, or data targets
- Provide data for forensic/post-mortem analysis if an incident does occur
- Serve as proof of effective controls on business critical information

Tools to help with this: SQL Server does provide native C2 auditing to help with gathering this information. However, C2 auditing can be very resource intensive and does not provide fine-grained controls to let you specify what you want to collect. You may instead want to use a 3rd party auditing tool, such as Idera **SQL compliance manager**. **SQL compliance manager** provides customizable, low-impact auditing, alerting and reporting on virtually all activity across multiple SQL servers.

10 steps TO SECURE YOUR SQL SERVER

step 8

AUDIT THE ACTIONS OF ADMIN USERS ON YOUR SQL SERVERS

Even after an extensive search to find a trusted babysitter, many parents still make unannounced visits home, or even install webcams to find out what is really happening while they are away. The same goes for power users on your SQL Servers – even if you trust those with system administrator privileges, it's still a very good idea to keep a record of what they are doing. In other words, trust, but verify.

DBAs with system administrator privileges are omnipotent within their SQL Server realm. They can access any and all data without an audit trail. Additionally, they can create logins, change permissions, and restructure data models. Thus, creating a record of system administrator activity is critical for compliance auditing, change control, and general peace of mind.

Tools to help with this: The native SQL Server C2 auditing can also be used for this purpose, however, there is no way to ensure an immutable trail of audit data with the native tools. So, what's to stop an admin user from deleting the audit trail after making off with your customer list? A better solution is to invest in a 3rd party tool such as **SQL compliance manager** which can audit ALL admin user activity, and protect the audit trail from tampering by anyone, even admin users.

step 9

SECURE AND AUDIT THE APPLICATIONS THAT ACCESS YOUR SQL SERVER DATABASES

Software vulnerabilities often provide the conduit for database attacks or data theft. To use the house analogy again, the doggie door for your favorite pooch can provide a crook easy access to your home. As a result, applications involved in performing core business functions, most often financial, need to have some sort of audit trail to comply with regulations and to track user activity for security, productivity, or other considerations.

10 steps

TO SECURE YOUR SQL SERVER

To ensure security in this area, make the following best practices a part of your business:

- Follow secure coding practices – a high percentage security issues can be traced to coding problems
- Control access (authorization) within the application.
- Encrypt login IDs and passwords.
- Use a proven authentication model that matches your business and security needs. Consider whether users are external, internal or both. For example you don't want to create internal domain accounts to authenticate external users.
- Always validate user input - Check for proper input data, length, type, etc. Many attacks take advantage of non-validated fields to execute malicious code.
- Implement application audit trails – if you can't audit activity, how can you detect unusual behavior, or conduct forensic analysis if a security issue occurs?

Tools to help with this: Idera **SQL compliance manager** will track the activity of any application within a targeted database. And, alerts can be configured to watch for and provide immediate notification of questionable behavior, such as a business application accessing a database it shouldn't.

» step 10

ENSURE PROPER DATABASE BACKUPS, AND SECURE YOUR BACKUPS

Bad things happen. It's usually not a case of "if", but of "when". Just like you carry insurance on your house, a well thought out database backup plan is an insurance policy for your business. Without an effective backup and recovery plan, you risk permanent loss or theft of business data, source code, product plans, customer lists, patient data, credit card information, and more.

A good insurance policy ensures you have the ability to recover from any security (or other) mishap, thus you need complete and timely backups. It is highly recommended that you test your backup files and recovery process. Familiarity with the restore procedures will help you quickly recover in the case of a failure.

Additionally, the backup files must themselves be protected. Backup files contain all your data, and stolen backup copies represent a huge security breach. Protect these files with file system security as well as encryption if the data is of high value.

Tools to help with this: While SQL Server does give you the ability to backup your databases, it does not include the ability to encrypt the backups, or compress them to help save space and reduce backup time. Idera **SQLsafe** provides a high performance backup solution which includes encryption and compression. **SQLsafe** also lets you create backup policies with exception reporting to notify you of any backups that failed to run as scheduled.

All of Idera's Tools for SQL Server, including those for compliance and security, can be downloaded free for 14-days. Visit **www.idera.com** for more information.

idera™
TOOLS FOR SQL SERVER™

10 steps TO SECURE YOUR SQL SERVER

SQL SERVER SECURITY RECOMMENDATION	RECOMMENDED TOOL
Keep systems up to date on Service Packs, Patches, and new versions of the OS and SQL Server	Idera **SQLsecure** collects SQL Server version number and service pack as part of the overall security assessment it performs. The version number returned by **SQLsecure** will also reflect the latest patches applied, so you can determine which servers are out of date.
Enforce standards for secure passwords	If you are using SQL Server 2005, use the built-in security options to enforce password complexity standards. For previous versions of SQL Server, there are many publicly available scripts you can use to identify accounts with weak or non-existent passwords
Secure the full environment, including the OS and Network	Microsoft has many documents and knowledge base articles that provide more detail and best practices on how to ensure server and application security.
Ensure appropriate SQL Server Setup	Idera **SQLsecure** checks key security settings across your SQL Servers and reports back where you have potential security concerns.
Regularly assess WHO can access your SQL Servers and take action to limit access	Idera **SQLsecure** automatically generates a complete list of all users with access to your SQL Server, across Windows, Active Directory, and SQL Server, including users that have access as a result of group membership.
Assess what actions users can perform on what objects	Idera **SQLsecure** calculates both effective (derived) and assigned permissions for all users, on any database object, making it much easier to ensure that users have appropriate access rights.
Keep an audit trail of database activity	Idera **SQL compliance manager** provides customizable, low-impact auditing, alerting and reporting on virtually all activity across multiple SQL servers.
Audit the actions of Admin users on your SQL Servers	Idera **SQL compliance manager** audits ALL admin user activity, and protects the audit trail from tampering by anyone, even admin users.
Secure and audit the applications that access your SQL Server databases	Idera **SQL compliance manager** will track the activity of any application within a targeted database, and alerts can be configured to immediately notify you of questionable behavior.
Ensure proper database backups, and secure your backups	Idera **SQLsafe** provides a high performance backup solution which includes encryption and compression. **SQLsafe** also lets you create backup policies with exception reporting to notify you of any backups that failed to run as scheduled.