SQL Server Security

03/30/20172 minutes to readContributors all

In this article

SQL Server has many features that support creating secure database applications.

Common security considerations, such as data theft or vandalism, apply regardless of the version of SQL Server you are using. Data integrity should also be considered as a security issue. If data is not protected, it is possible that it could become worthless if ad hoc data manipulation is permitted and the data is inadvertently or maliciously modified with incorrect values or deleted entirely. In addition, there are often legal requirements that must be adhered to, such as the correct storage of confidential information. Storing some kinds of personal data is proscribed entirely, depending on the laws that apply in a particular jurisdiction.

Each version of SQL Server has different security features, as does each version of Windows, with later versions having enhanced functionality over earlier ones. It is important to understand that security features alone cannot guarantee a secure database application. Each database application is unique in its requirements, execution environment, deployment model, physical location, and user population. Some applications that are local in scope may need only minimal security whereas other local applications or applications deployed over the Internet may require stringent security measures and ongoing monitoring and evaluation.

The security requirements of a SQL Server database application should be considered at design time, not as an afterthought. Evaluating threats early in the development cycle gives you the opportunity to mitigate potential damage wherever a vulnerability is detected.

Even if the initial design of an application is sound, new threats may emerge as the system evolves. By creating multiple lines of defense around your database, you can minimize the damage inflicted by a security breach. Your first line of defense is to reduce the attack surface area by never to granting more permissions than are absolutely necessary.

The topics in this section briefly describe the security features in SQL Server that are relevant for developers, with links to relevant topics in SQL Server Books Online and other resources that provide more detailed coverage.

In This Section

Overview of SQL Server Security
Describes the architecture and security features of SQL Server.

Application Security Scenarios in SQL Server
Contains topics discussing various application security scenarios for ADO.NET and SQL Server applications.

SQL Server Express Security
Describes security considerations for SQL Server Express.

Related Sections

Security and Protection (Database Engine)
SQL Server Books Online security topics.

Security Considerations for SQL Server
SQL Server Books Online security topics.

See Also

Securing ADO.NET Applications
SQL Server and ADO.NET
ADO.NET Managed Providers and DataSet Developer Center