


The 'Must Haves' of Database Security

Teradata provides security controls to ensure compliance with security standards, policies, regulations and legislation.

by Jim Browning



The security, privacy and protection of database assets are increasingly important to organizations. To that end, the Teradata® Database provides a rich set of security features and controls that can be used to implement a comprehensive data security strategy.

The features ensure that users can access only the database objects for which they have been authorized. Controls make sure that all sensitive data is fully protected and access to it is effectively audited and monitored. The database capabilities fall under four main categories that are needed for effective data security.

Authentication

Authentication allows the database to securely verify a user's identity before allowing any access to database objects. A fundamental security best practice is to ensure that all users are uniquely identified and authenticated

using strongly constructed credentials. The Teradata Database provides options for both internal and external authentication of users.

Passwords for logging into the database must use a combination of alpha, numeric and special characters.

Security features in the database are integrated with corporate lightweight directory access protocol or Kerberos-based authentication systems. This allows for the centralized management of database users to be consistent with the management of users for

other systems and applications within an enterprise.

In addition, the **Trusted Sessions** feature in the database is used to assert end-user identities and roles through middle-tier, application-pooled connections. These identities can then be used for access rights and checking and auditing queries submitted by the middle tier on behalf of an end user.

Teradata Wallet can be employed to securely store and protect passwords. This eliminates the need to store passwords in clear text in scripts, **Teradata Parallel Transporter** operator definitions or within an open database connectivity data source name.

The database can also enforce IP filters to lock down privileged user accounts to only the applications, load/export systems and backup/archive operations for which the accounts have been authorized. This provides additional protection in the event an account is compromised.

Authorization

The “principle of least privilege” requires that a user be granted the minimum level of access required for his or her job. The Teradata Database supports a discretionary access control policy that is implemented with an extensive, granular set of rights and privileges that allows users to be given only the access needed to perform specific operations on particular database objects. Proper management of these rights is critical to prevent unauthorized or inappropriate access.

The Teradata Database handles this by using security roles to authorize database access rights by application, job description or responsibility. This

authorization can significantly reduce the complexity and cost of security administration in large database environments and also allows for security management at a level that closely corresponds to an organization’s structure.

**The Teradata®
Database allows
businesses to assess,
implement and
maintain strong
security measures that
are consistent with
industry best practices.**

Row- and column-level controls are used by the database to further restrict access to selected information in database tables. Column-level security restricts access to specific columns, while row-level security filters access to rows based on the identity of the user submitting queries.

Data Security

Sensitive information can be vulnerable when transmitted over non-secure networks or when appropriate access controls have not been enabled. Moreover, compliance with some standards and regulations requires encryption to secure the data during transmission and when it’s stored. The Teradata Database supports strong

encryption through industry-standard cryptographic algorithms and securely generated encryption keys.

Network traffic encryption protects the confidentiality of sensitive information when it’s transmitted over any public or untrusted network. It also protects the data from being compromised by network “sniffers.”

The database also lets organizations employ column-level encryption or tokenization to secure information stored in tables. This helps protect sensitive data from both internal and external threats, including being compromised by privileged database users.

Disk and tape archives containing sensitive information can be encrypted before they are transferred to an offsite or commercial storage facility. This removes the possibility of the data being at risk if the archives are lost, stolen or misplaced.

Auditing and Monitoring

Teradata Database audit logging facilities assess different kinds of security events to detect possible security violations, such as attempts to compromise a user’s login, unauthorized attempts to access database objects or changes to the logging rules. Access log rules can be configured to audit all access to sensitive data and all operations performed by privileged database users.

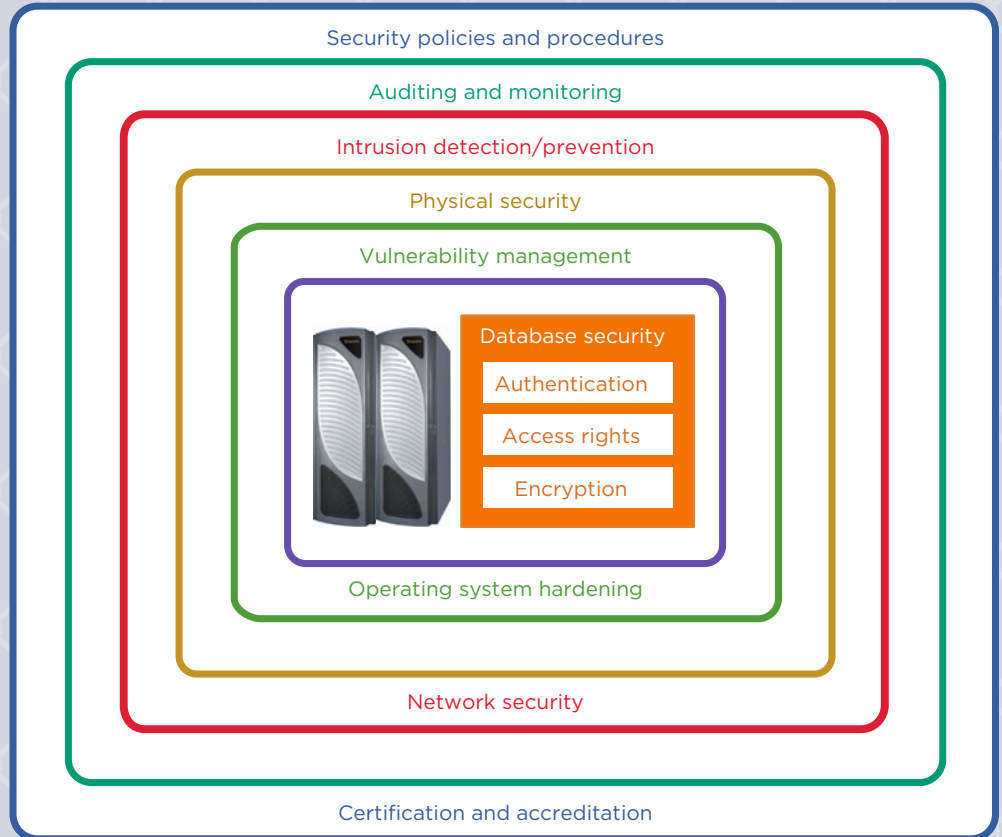
A security administrator can configure the system to log any combination of access requests, requests denied or specific types of requests for any or all users. The log records can include the SQL expression that was used to perform the access,

MULTIPLE LAYERS OF SECURITY

Defense in depth is a strategy that involves implementing multiple layers of security defense mechanisms to protect critical business data. If a single layer or mechanism fails or is compromised, other layers ensure the security of the data.

The security layers take multiple forms. Some include a company's security policies and standards, others include the procedures to manage and monitor system access, while still others are implemented as technological controls. It is important to recognize that there is no one layer or set of controls that can be implemented to fully and properly secure a database system.

FIGURE Defense in Depth Security Framework



whether indirectly through views or directly to base tables.

Companies can use database features to regularly monitor all audit logs. This helps ensure that users are performing only activities for which they have been explicitly authorized. The frequency of reviews should be determined by risk factors such as the criticality of the database to business operations, the value or sensitivity of the information stored in the database, past issues with system compromises or misuse of information and the extent to which

the system might be accessible via non-secure networks.

The database gives organizations the ability to periodically archive all audit logs for use in security investigations or forensic analysis. If a breach is detected, the availability of the audit logs is critical to determine the source.

Critical Security Components

The Teradata Database allows businesses to assess, implement and maintain strong security measures that are consistent with industry

best practices. A properly protected database is one essential component of a comprehensive security strategy, and features in the Teradata solution provide the critical components to safeguard the data. **T**

Jim Browning is the enterprise security architect for Teradata Labs.

ONLINE

This article is based on the white paper "Security Features in the Teradata Database." Download it on Teradata.com.