

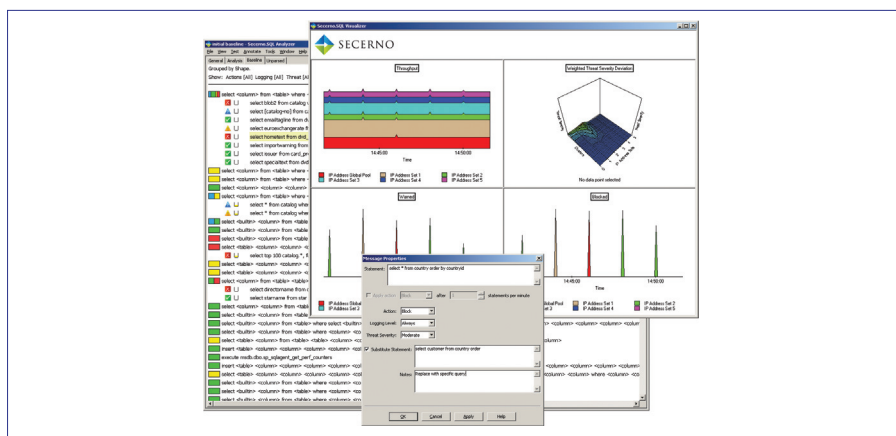
Database security from Secerno.SQL

The increasing requirements for compliance with data security regulations mean that companies can no longer afford to risk their futures by ignoring their databases. In response to this, we are seeing a number of database security products emerging and Secerno.SQL offers an unusual solution. It is exceptional, in that it incorporates built-in intelligence, creating a defensive perimeter around either Oracle or SQL Server databases, thereby protecting against internal and external threats.

Secerno.SQL is appliance based and the Assurance model - on review - is aimed at mid-sized organisations. It offers deep inspection capabilities at Layer 7 (application level), analysing SQL statements to determine real-time database activity, establishing a complete picture of user behaviour and applying its intelligence to decide what activities are acceptable.

For the purposes of testing, we used systems running SQL Server 2000 and SQL Query Analyser, and found that the appliance is capable of monitoring DBMS traffic almost immediately. Two deployment scenarios are supported: passive and enforcement. Operating in a passive IDS (Intrusion Detection System) mode, the system analyses traffic using a spanned switch port, allowing it to log DBMS traffic and report on activity, but it cannot block anything.

To enforce security policies, the appliance is placed in-line where the data flows through it in enforcement mode. This IPS (Intrusion Prevention System) mode allows it to provide a number of functions with SQL statement substitution at the top of the list. Secerno.SQL is highly versatile, as you can change the contents of specific statements as they pass through the appliance. If any statements are deemed a



threat, then the appliance will block them (although the default method isn't elegant, as it merely performs TCP resets). However, it is possible to substitute an SQL query with another benign statement, which produces error codes that the requesting application can deal with gracefully.

The network must be baselined, so you place the appliance in a training mode where it collects and stores all SQL statements. It will even tell you when it's safe to switch off training, as it uses a 'degree of completeness' metric, based upon new data and database change frequencies. The collected data is then downloaded to the SQL Analyser utility, where it organises statements of similar intent into clusters and cluster groups.

Each statement, or cluster, is assigned an action and the Analyser handles this automatically, as it can determine threat levels and assign each one with a threat severity, logging level and action. These decisions can be reviewed and modified and, if it all looks good, then you create a baseline and upload it to the appliance.

Clearly, database security policies can be deployed very swiftly and, as new SQL statements are identified, you may decide to block, warn or pass them; or just leave

them unassigned for you to review.

By leaving the training mode on, you can tweak your policies as time goes by and user activity changes. The collected information is downloaded to the Analyser, where colour coding makes it easy to identify new statements. You can leave the Analyser to decide the best policy for them, or assign your own actions and threat levels, and then upload the new baseline. Now that the appliance has a clear idea of database activity, it can block unusual traffic and log suspect user behaviour. For the latter, this could range from a user requesting unusually large amounts of records, accessing areas of a database or tables they normally don't use, or running queries at unusual times.

Secerno.SQL is a simple, yet sophisticated, answer to the growing problem of database security. It's remarkably easy to deploy and manage, and can implement very strong access policies, providing a wealth of information about database activity.

Product: Secerno.SQL
Supplier: Secerno
Telephone: 0845 450 9460
Web site: www.secerno.com
Price: From £20,000

Verdict: Secerno.SQL is a simple, yet sophisticated, solution to the growing problem of database security. It is unusual, in that it incorporates built-in intelligence, creating a defensive perimeter around either Oracle or SQL Server databases, thereby protecting against internal and external threats. It's also remarkably easy to deploy and manage, and can implement very strong access policies