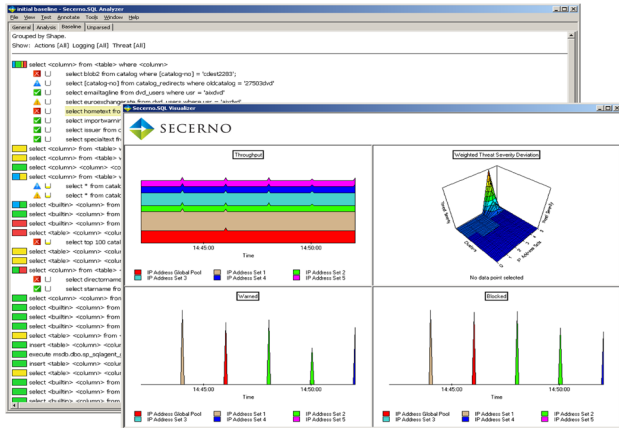


« Database security

Secerno.SQL



Supplier Secerno
Price From £20,000 excluding VAT
Contact www.secerno.com

Database security is never far from the news as businesses persistently fail to provide adequate protection for their customer data. UK-based Secerno was founded in 2004 with a very clear focus on this area. The Secerno.SQL Assurance appliance delivers a unique solution for monitoring, analysing and logging database usage and enforcing security policies.

As the appliance inspects database management system (DBMS) traffic at the layer 7 application level it can gather a great deal of information. It identifies and analyses all SQL statements and determines precisely what database activities are occurring in real time. It builds up a detailed picture of usage, allowing it to spot unacceptable behaviour. Any unusual traffic can be automatically blocked and suspect user behaviour logged and highlighted for further investigation. At present, only Oracle and SQL Server are supported, separate appliances are needed for each type and alerting is limited to syslog.

Using test systems running SQL Server 2000 and the SQL Query Analyser we found installation very simple as the appliance can start

monitoring DBMS traffic straight away. It supports two distinct modes of operation and, in IDS mode, sits to one side and monitors database traffic via a spanned port on a network switch. This is entirely passive as the appliance logs database traffic but cannot block access. Note that Secerno only requires half-duplex port-spanning as it is just interested in traffic coming into the database and does not interact with outbound traffic.

In IPS mode, the appliance is placed directly in line of database traffic, allowing it to offer a number of extra security functions. The most valuable is its ability to perform statement substitution as it can change the contents of SQL statements on the fly. This has a multitude of uses as you could, for example, change a request from a user asking for credit card information to return the numbers and user details obscured. When suspect SQL statements are identified access can be blocked, although the appliance merely performs a TCP reset.

The device starts in a training mode, where it logs database traffic over a period of days or weeks to get a clear picture of how the databases are being used.

To create a baseline you download the data collected by the appliance to Secerno's SQL

Analyser tool, which opens with a complete rundown of every SQL statement captured. These are listed under the analysis tab and the software gathers statements with similar meanings into clusters and groups. A small pie chart shows their frequency, and you can change to views of selected tables, columns, IP addresses or database users.

Moving to the baseline tab shows all SQL statements and what actions have been assigned to them. The Analyser can determine the threat level posed by each statement and automatically assign a threat severity, logging level and action. You decide how to handle new SQL statements as the appliance can be set to block, warn or pass them, or leave them unassigned. Once you're happy with the settings you create a baseline, upload it to the appliance and you're up and running.

Your baseline can be fine-tuned by leaving the training mode on to allow the appliance to gather more data. Colour codes for each action make it easy to see new entries and you can let the Analyser decide what to do with them or assign actions yourself. You can add custom SQL statements to the collection and assign actions to them to pre-empt specific activities.

The appliance's web interface groups multiple appliances into sets for easier management. It provides views of outstanding tasks plus stored baselines and lets you upload new baselines. The traffic snapshot will prove useful as it provides four graphs offering a real time rundown of statements



being blocked and warned, statement throughput and the most frequently blocked clusters. The Visualiser tool adds considerable value as it provides a dashboard of graphs showing real-time activity.

We found the Secerno.SQL appliance simple to use and were impressed with the amount of information it can gather. It's a unique solution that provides an in-depth view of how databases are being used and the tools to ensure they are protected from misuse and attacks.

Dave Mitchell

SC MAGAZINE RATING	
Features	★★★★☆
Performance	★★★★★
Ease of use	★★★★★
Documentation	★★★★☆
Support	★★★★★
Value for money	★★★★☆
OVERALL RATING	★★★★☆
For Very swift deployment, detailed logging, intelligent security policy creation, attacks and abnormal user behaviour easily detected once baseline created	
Against Oracle and SQL Server databases require separate appliances, syslog support only	
Verdict A sophisticated solution that's swift to deploy and easy to manage	

Contact details:



United Kingdom

Seacourt Tower
 West Way
 Oxford
 OX2 0JJ

Telephone: +44 (0)845 450 9460
 Email: enquiries@secerno.com
 Web: www.secerno.com