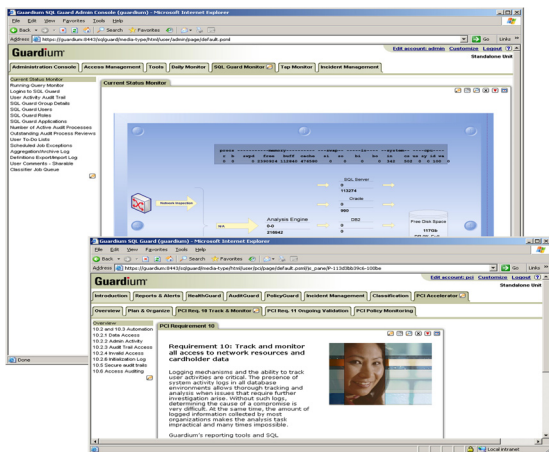


« Database security

Guardium Monitoring and Security Suite 6



Supplier GuardiumUK
Price From £25,000 excluding VAT
Contact www.guardium.com

There is a growing range of database security solutions on the market. Guardium's Database Monitoring and Security Suite 6.0 provides an extensive range of security measures that allow companies to monitor and audit database usage and enforce policies to prevent unauthorised access. It monitors database management system traffic at the network layer and is deployed as a 1U Dell PowerEdge 1850 rack-mount appliance. On review is the SQL Guard Network Monitor device, which monitors database traffic via spanned ports on network switches.

Guardium also offers an SQL Guard Database Firewall suited to large remote installations that require local database firewalling and access control. Big distributed networks with multiple appliances can use a central manager appliance to maintain them. Lastly, there's the Guardium network monitor, a software probe aimed at small remote locations, where switch port spanning is not possible and no appliance is required.

For testing we employed Supermicro dual 3GHz Xeon 5160 servers with Oracle 10G R2 and MS SQL Server 2000 and used XP

SP2 client systems running SQL+ for Oracle and the Query analyser for MS SQL Server. Guardium requires ingress and egress port spanning, and we had a problem with our HP ProCurve 2848 Gigabit switch as it doesn't appear to support full duplex modes. To get round this we installed Guardium's software probes on our database systems.

The appliance delivers an intuitive web interface and monitors database traffic straight from the box. You choose what inspection engines should run from options including MSSQL, Oracle, Informix, DB2 and Sybase. This includes FTP and Windows file sharing and it can monitor many proprietary protocols such as named pipes and Oracle Bequeath.

Access is determined strictly by user roles and a key differentiator is that Guardium does not allow root access to the appliance. This is valuable for regulatory compliance as the data and reports held on the device cannot be modified. Furthermore, the appliance maintains an internal audit showing who logged on to it and what they did. Global settings are applied to each inspection engine, and the default style for reports is to show SQL queries without their values. This tightens security even further as reports won't show sensitive information unless instructed to do

so. Incident management allows multiple occurrences such as login failures to be grouped together.

Alerting is simplified, as specific incidents can be used to notify selected users. Each incident is assigned to specific users who can add comments, change its status and close the resolved incident.

We liked the fact that the web interface can be customised. A preconfigured interface is provided for PCI (payment card industry) compliance. Report creation for all roles is easy as you can use existing ones as templates. Aliasing allows reports to show what database components systems are running rather than giving their IP address.

You can review reports and pass them to other users for approval and sign-off. The latter function is handled by the AuditGuard module, and once a report has been signed by a user they cannot modify or remove it.

The PolicyGuard component needs the appliance to baseline the network first. It automatically identifies database-related traffic, captures these packets, analyses their contents and stores the results. Baselining allows PolicyGuard to build a picture of the network and suggest rules based on its findings.

Access rules are used to monitor database users and report on their activities. If unauthorised activity is spotted the rule takes action, ranging from sending an alert to terminating user access. Appliances in span-port mode can issue TCP resets, while the firewall model terminates at the SQL-command



level. Extrusion rules look at data exiting a database so can see the results of user queries and check for patterns such as credit card numbers. The appliance can use external data sources and integrates with the Remedy change management solution, allowing you to stop users making schema changes without a valid ticket.

Guardium provides a sophisticated database security solution that is simple to install and deploy. Businesses have a legal duty to protect their customer information, and this has the tools to ensure they meet regulations.

Dave Mitchell

SC MAGAZINE RATING	
Features	★★★★★
Performance	★★★★★
Ease of use	★★★★★
Documentation	★★★★☆
Support	★★★★☆
Value for money	★★★★☆
OVERALL RATING	★★★★★

For Easy installation, massive database support, sophisticated reporting, strong policy-based security, PCI out of the box
Against We encountered problems with HP ProCurve switch port spanning
Verdict If you're not sure whether your databases are secure, check out Guardium as it's smart enough to keep your business on the right side of the law

Contact details:

Guardium
SAFEGUARDING DATABASES™

Email: info@guardium.com
 Tel: (0)207 1524094 (UK) or +1 781.487.9400 (US)
 Web: www.guardium.com