**Database administration security strategy.Given the vital importance of the information held within corporate and government databases it is surprising that the security of these databases is often of unknown provenance, at least as far as those charged with information security duties are concerned.**I am not setting out to offend an entire section of the IT industry by picking on database administrators. However, I believe database administrators and security managers need a better mutual understanding so that the security of these vital resources can be improved without overly database performance.One of the common refrains I hear from database administrators is that they are unable to implement security mechanisms as the associated performance hit is too high. It is not my intention to explore the various intrinsic [database security mechanisms](http://searchsecurity.techtarget.com/buyersguide/Database-security-products-A-buyers-guide) or to discuss their strengths and weaknesses. My purpose here is to suggest methods of securing information while shifting the burden of securing databases from the administrators and not excessively impacting performance. Over the past couple of years, the mysteries of database security have been brought towards the mainstream of information security. This move towards the mainstream is in part due to the increased focus of talented security researchers on the security of databases. Their work has highlighted a number of vulnerabilities within the well-known database products ranging from design flaws through to traditional buffer overflows within the database applications themselves. Unfortunately, their work has also identified that database suppliers are not, in general, as diligent in patching as the major operating systems suppliers. Technology, although it is not the whole answer, can help to secure databases. For example, companies such as Guardian and Secerns offer database firewalls that control the traffic flowing to and from databases based on a comprehensive understanding of the underlying database communications. These tools understand the SQL statements being passed to the bac-end database and can reject those that are considered dangerous. If the thought of a relatively immature technology making access decisions that could prevent your mission-critical systems accessing the information they rely upon is a little disturbing, then you could use these tools in a monitoring mode until confidence levels increase. Alternatively, a database audit trail that is completely outside the control of the database administrators may itself be the goal it certainly provides a greater degree of separation of duties than relying on the intrinsic database audit functionality. In addition, a number of tools for performing automated security audits of databases are available. They cater for the common flavors of database and provide comprehensive reports of security vulnerabilities together with suggested remediation activities. Taken in conjunction with a baseline of good practices, including database and host hardening, appropriate vetting of database administrators, effective user management, and patching, the tools discussed here can help to reduce the risks of one of your most precious assets - your information - being compromised through poor or untested database security measures.