G00226793

Establishing a Strategy for Database Security Is No Longer Optional

Published: 29 November 2011

Analyst(s): Jeffrey Wheatman

The options for securing increasingly valuable databases are very broad and deep, and can be confusing. This research provides an overview of three categories of controls that should be implemented to ensure that enterprise data is protected in the most efficient and effective manner.

Key Findings

- Databases continue to grow in size, complexity and importance, while enterprises struggle to identify the most appropriate controls regarding their use and misuse.
- There are limits to many of the preventive controls that are being used to keep out individuals who should not have or don't need access.
- The most effective database security implementations will leverage controls across administrative, preventive and detective controls. Balance is critical to get maximum protection with limited budget and head count.
- Relational database management system (RDBMS) vendors have gotten better with native security controls and add-ons, but third-party tools generally provide the best balance of security, usability and cost.

Recommendations

- Evaluate the current state of enterprise database security. Identify gaps, and look for opportunities to close them.
- Integrate database security with data security policy and governance directives.
- Implement detective controls to address risks associated with the inability to implement comprehensive preventive measures.

What You Need to Know

The importance of database management systems (DBMSs) continues to grow. The current volume of data stored in DBMSs continue to increase at a rapid rate, and the increasing complexity of the systems makes it more difficult to secure than ever before. DBMS vendors have come a long way in providing more secure platforms for system deployment, and there are many vendors and tools that can enhance the security of databases, but securing DBMSs has not gotten significantly easier.

There are numerous drivers for the growth of DBMSs, most notably:

- Database migration
- Data warehousing
- Consolidation of databases
- Data retention and e-discovery
- Advent of big data

Unfortunately, the security controls for databases and DBMSs have not kept pace with increasing risks.

It is also important to note that there has been an increase in focus on nonrelational data stores, and this model and the traditional approach must be adjusted for these systems.

Analysis

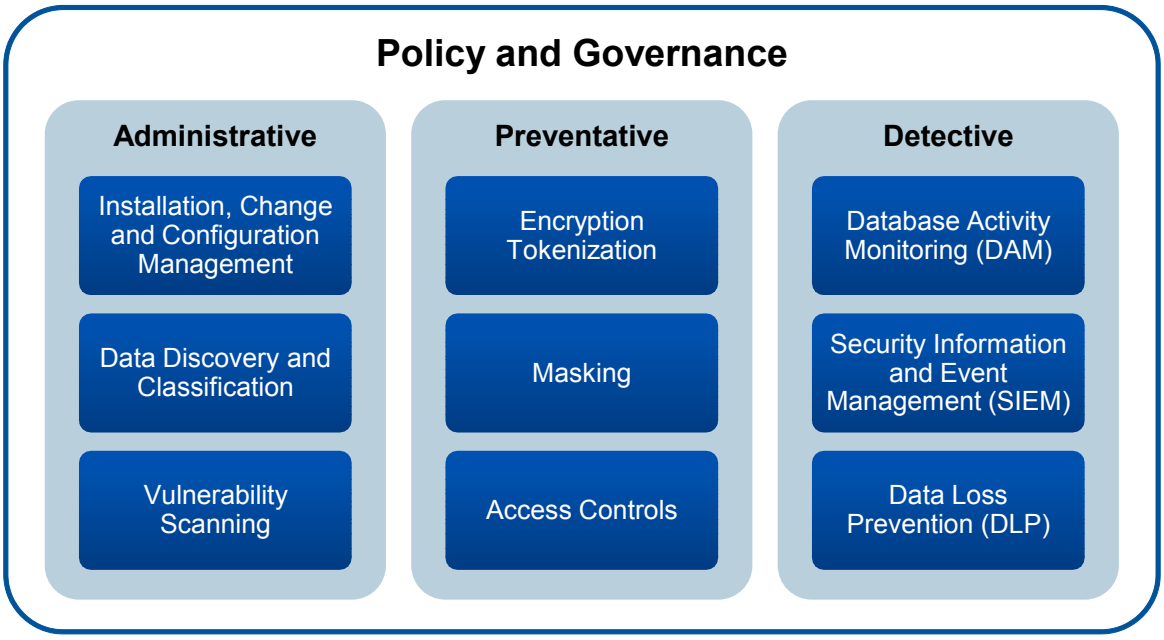
Context

The guidance in this research is applicable to clients that store regulated or data otherwise defined as "business critical" within RDBMSs.

Analysis

To help clients properly secure their relational databases, Gartner has developed a model for database security (see Figure 1).

Figure 1. Gartner's Database Security Model



Source: Gartner (November 2011)

The First Step: Governance and Policy

An effective security governance process is a key precursor to the most basic decisions about the implementation of processes or tools. Sound data security governance must be integrated with overall IT and information governance initiatives, requiring that the enterprise's security and risk management leaders be involved in risk decision making.

Once these foundational decisions have been made, they must be translated into policies that are realistic, reflect the enterprise's business drivers, and are targeted at the appropriate stakeholders. For example, a policy for protecting the enterprise's intellectual property (IP) must describe the processes supporting the policy; define the IP; detail the business, technical and security requirements to be considered; describe the tools to support the requirements; and show how the tools will be implemented and managed. Whatever controls are selected, the control objectives and targets must be linked back to the enterprise's classification schema.

Administrative Controls

Installation, Change and Configuration Management

Default installation of a DBMS is geared toward ease of installation, rather than security. As much as focus on security has increased during the past few years, Gartner still sees inconsistently applied hardening at the data storage layer. Common risks are:

- Default privileged user account settings
- DBMS installed using standard configuration
- Sample scripts and code left in place

DBMS vendors provide security guidelines and may provide hardening scripts that can be run after installation. Numerous third-party guides (see Note 1) provide guidance for securing your systems, although they tend to be stricter than the vendor guidelines, and all changes should be tested to ensure operational viability.

Deploying a secure system is only the first step. Ongoing change and configuration management continue to be critical and are often not done very effectively, leaving systems in inconstant and unsecure states.

Best Practices:

- Harden systems at all layers, customize security configuration by function, and define patching procedures.
- Integrate DBMSs into your threat and vulnerability management process.
- Develop a release management process for business-critical systems.

Data Discovery and Classification

As the volume of enterprise data expands at an ever-increasing rate, it becomes more difficult to locate and classify data as part of a data protection program. There are still huge volumes of data and individuals and applications that provision storage that are not always consistent in naming conventions or formats. Locating, categorizing, classifying and valuing data contained in DBMSs are important prerequisites for securing it.

Best Practices:

- Discover RDBMSs — stand-alone systems, as well as those part of business systems.
- Locate your critical data within your databases. Clarify data types that need to be protected because of business requirements, and legal and regulatory mandates.
- Leverage data discovery tools wherever possible.

Vulnerability Scanners

Vulnerability scanning tools are an integral part of a threat and vulnerability management program, and will support enterprise goals for database security. These tools use active and passive mechanisms to locate known vulnerabilities, common misconfigurations and other weaknesses. There are tools that focus specifically on databases, but it is common to use network or application scanners. Scanning tools function by sending attack and probe packages against the database

and, in some cases, the underlying operating system by using agent-based technology to evaluate database configurations and parameters.

Some of these tools integrate with database activity monitoring (DAM) or security information and event management (SIEM) as part of a comprehensive vulnerability management program.

Best Practices:

- Leverage current vulnerability scanning tools for databases.
- Evaluate whether the deployment of a dedicated DBMS scanner tool will give you better results, but ensure you can manage extra remediation.
- Use scanning to support change and configuration management program goals.

Preventative Controls

Encryption

Early versions of encryption tools often required the entire database to be encrypted, leading to performance degradation and broken applications. In addition, the data was not hidden from administrators. Most DBMS vendors now offer native encryption at the database, table and field levels, and prevent administrators from having access to keys. There are also third-party encryption tools that provide a single point configuration and key management.

It is important to understand that, although encryption can be a strong control, it does have limitations. Encryption is good for enforcing segregation of duties and keeping data out of the hands of unapproved users. And it can be used to protect data as it moves from one place to another (for example, backing up data). But, it won't help if roles are not clearly defined. For example, if the user is given a role that is not appropriate, he will have access to the keys, and it won't prevent inappropriate use of legitimate access, such as downloading thousands of records.

Tokenization is a subset of encryption that involves substituting "tokens" for real data and removing the data to be protected from areas where they would be easily accessible. Tokenization can be helpful in protecting easy-to-define data, such as credit card numbers or Social Security numbers in the U.S. It can, however, be challenging to leverage tokenization for data such as privacy and healthcare data, which tends to be more difficult to define.

Best Practices:

- Assess your DBMS platforms, and evaluate what options may be available from your DBMS vendors.
- Educate stakeholders on the benefits and limitations of encryption tools. Encryption has become a "go to" for legal and regulatory scenarios but does not always address risks appropriately.

- Test encryption solutions in a lab environment before deploying in production to ensure they won't break your applications.
- Evaluate tokenization for discrete, easy-to-define data types, such as credit card numbers or Social Security numbers.

Data Masking

Masking technologies help prevent sensitive data from being exposed to unauthorized individuals by replacing it with realistic substitute data. This is a data security protection that is often recommended by regulatory bodies and legal requirements — for example, PCI and the Health Insurance Portability and Accountability Act. Data-masking technology takes two basic forms:

- Static masking aims to prevent the misuse of data by users of nonproduction databases by masking data in advance of testing.
- Dynamic masking is an emerging technology that aims to mask data in real time, typically in production databases.

Best Practices:

- Consider using static data masking to limit access to sensitive data by employees (such as programmers, testers and database administrators [DBAs]) during development and testing.
- Begin to look at dynamic data masking for use cases (such as in call centers), as the technology matures.

Access Management

Once your DBMSs are deployed and configured, ensure that your access controls are set appropriately at all layers — network, application and data. The ultimate goal, however impractical it may be, is to implement least privilege. In other words, allow only what is strictly necessary to get the job done. Identity and access management (IAM) offerings provide a key central access management locus. Several common vulnerabilities associated with access management are:

- Allowing connections directly to the database, rather than going through applications bypassing application controls
- Allowing connections from nonstandard applications, such as RDBMS tools
- Use of administrative credentials for "normal" work activity
- Poor mapping between business roles and technology access roles
- Depending on access control at one layer (for example, implementing only application-based access control)

Best Practices:

- Implement logical network segmentation and tiered architectures. Use access control lists to prevent unauthorized connections to databases.
- Deploy jump boxes for DBAs to conduct database administrative activities, and limit access to database tools such as Toad and SQLTools to approved DBAs.
- Require clearly defined access roles rooted in an IAM program. Review role membership and access controls to ensure that they match job requirements.
- Implement complementary access controls at the database layer. Don't depend only on application-layer access controls.

Detective Controls

Although there have been improvements in DBMS security options, organizations struggle to secure established DBMSs that were not designed with effective security controls. We have also seen an increased focus on data security resulting from regulatory pressures. Even if you follow all best practices above, there are still risks to your data:

- Data must be accessible to be used. Once data is accessible, it's at risk.
- Keeping up to date with patches is difficult.
- Encryption is a partial solution that has risks caused by key management issues and DBA access.
- A strong access control program can limit exposures, but role-based provisioning, especially in complicated systems, is difficult.
- Network segmentation and filtering will limit risks, but data must be accessible to be useful.
- None of the solutions above will prevent data disclosure to legitimate users with malicious goals.

These are controls that can and should be included in the database security program to ensure that risks associated with gaps in other protections are mitigated and that legitimate privileges are not misused. There are three primary detective controls that can be leveraged for database security.

Database Activity Monitoring

DAM controls analyze database activity to identify and report on fraudulent, illegal or other inappropriate behaviors, with minimal impact on user operations and productivity. When configured with knowledge of database structures, DAM can operate as an extension of DBMS audit functionality or independently. DAM has two primary use cases: (1) privileged user monitoring, focused on monitoring, analyzing and reporting on actions undertaken by users with high levels of access; and (2) application user monitoring, focused largely on database access that results from

transaction activity from the end users and applications that connect to the database. During the past several years, DAM tools have added a wider range of functions, such as:

- Data discovery
- Workflow and remediation management
- Prevention/blocking
- Vulnerability scanning
- Entitlement management

Best Practices:

- Implement DAM to mitigate the high levels of risk from database vulnerabilities, and address audit findings in areas such as database segregation of duties and change management.
- DAM technology should be used when a need exists for granular monitoring, or when the overhead of database audit functions is unacceptable.
- Implement DAM to monitor privileged-user access and access to critical data. Establish thresholds for "normal" behavior in your database and DBMSs.

Content-Aware Data Loss Prevention

Content-aware data loss prevention (DLP) tools address the risk of accidental exposure of sensitive data outside authorized channels, using monitoring, blocking and remediation functionality. They enable the dynamic application of policy based on the classification of content determined at the time of operation. DLP technologies are being increasingly leveraged for data discovery and classification purposes. These technologies perform deep-content inspection, using detection techniques that extend beyond basic keyword matching (for example, advanced regular expressions, Bayesian analysis and machine learning).

Best Practices

- Develop clear DLP strategies with concrete requirements before evaluating products.
- Understand the limitations of DLP within RDBMSs. DLP is a data-centric control and does not have any understanding of SQL, which is the primary mechanism for interacting with RDBMSs.

Security Information and Event Management

SIEM technology provides two primary data security capabilities: (1) log management (the collection, reporting and analysis of log data) and (2) security event management, which processes data from security devices, network devices, systems and applications in real time to provide security monitoring, event correlation and incident response. While SIEM is sometimes used for database security, SIEM deployments tend to be more device-centric and suffer from the same

gaps as DLP — not truly understanding SQL. Additionally, SIEM requires native DBMS logging to be turned on, resulting in increased overhead and management.

Best Practices:

- Define the requirements for data-centric compliance reporting, log management, resource access monitoring and security incident response. Product selection decisions should be driven by enterprise-specific considerations, including event management capabilities, capital and operations costs and support capabilities, and integration with established system and application infrastructures.
- Implement other monitoring solutions instead of or to complement DAM.

Key Facts

Databases continue to grow in size, complexity and value. However, the programmatic requirement to protect them has not kept pace. Database security still tends to be managed by DBAs and other technical resources, with a narrow view into the overall risk of the systems.

Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Best Practices in Change, Configuration and Release Management"

"Four Factors Driving Interest in Content-Aware Data Loss Prevention: A DLP Spotlight"

"Hype Cycle for Identity and Access Management Technologies, 2011"

"SIEM Enables Enterprise Security Intelligence"

"Key Trends in Securing Sensitive Data With Data-Masking Technologies"

"How to Identify Appropriate Controls for Enterprise Data Security Initiatives"

Note 1 Third-Party Database Hardening Guides

www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/database_servers.shtml

http://benchmarks.cisecurity.org/en-us/?route=downloads.browse.category.benchmarks.servers.database

http://iase.disa.mil/stigs/app_security/database/general.html

Regional Headquarters

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600