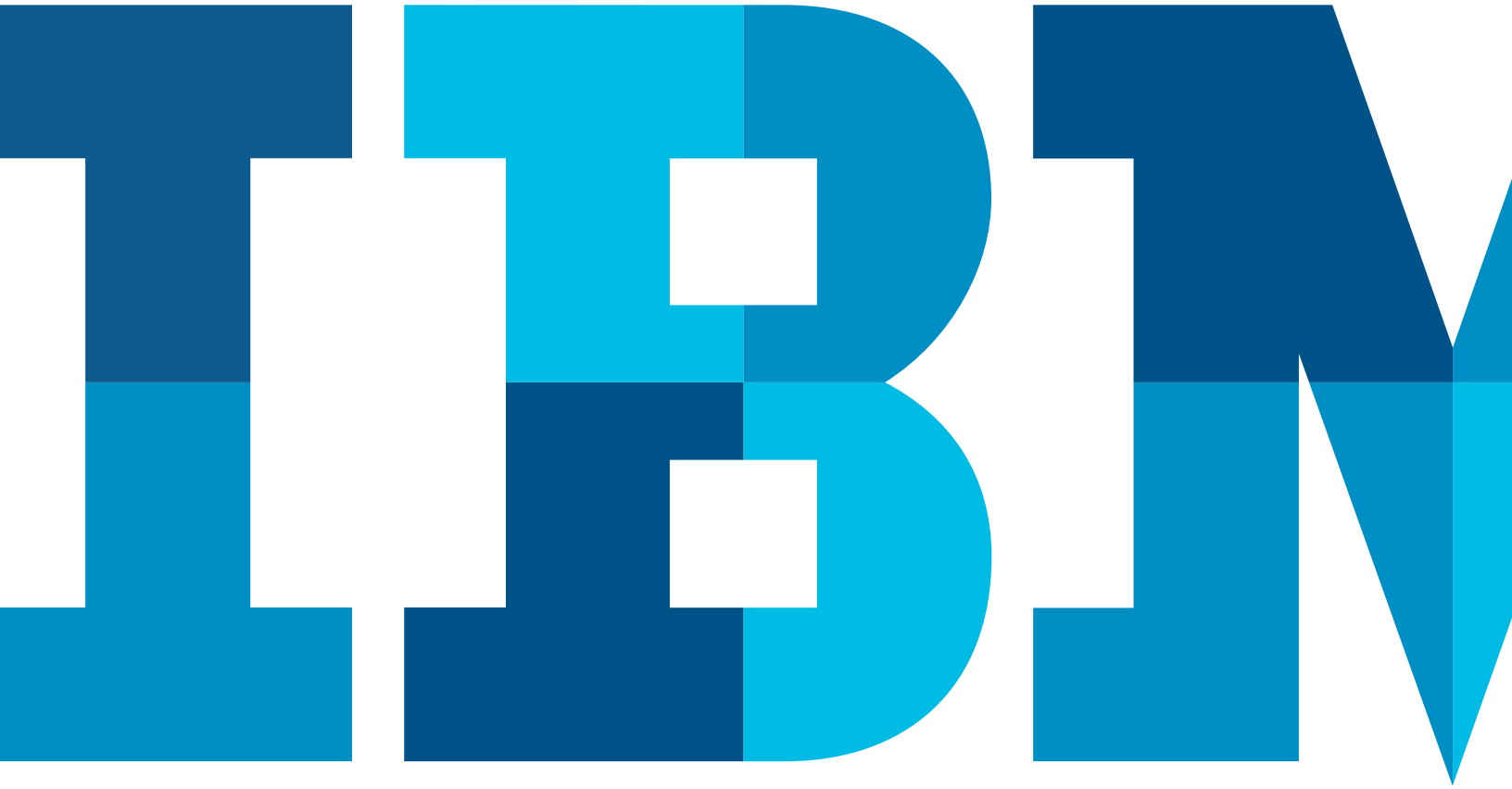
Information Management
White Paper

8 Steps to Holistic Database Security

By Ron Ben Natan, Ph.D., IBM Distinguished Engineer, CTO for Integrated Data Management



IBM

Cyberattacks, malfeasance by insiders and regulatory requirements are driving organizations to find new ways to secure their corporate and customer data found in commercial database systems such as Oracle, Microsoft SQL Server, IBM DB2 and Sybase. This paper discusses the 8 essential best practices that provide a holistic approach to both safeguarding databases and achieving compliance with key regulations such as SOX, PCI-DSS, GLBA and data protection laws.

Safeguarding databases and achieving compliance

Financially-motivated attacks, malfeasance by insiders and regulatory requirements are driving organizations to find new ways to secure their corporate and customer data.

Most of the world's sensitive data is stored in commercial database systems such as Oracle, Microsoft SQL Server, IBM DB2 and Sybase – making databases an increasingly favorite target for criminals. This may explain why SQL injection attacks jumped 134 percent in 2008, increasing from an average of a few thousand per day to several hundred thousand per day according to a recently-published report by IBM[1].

To make matters worse, Forrester[2] reports that 60 percent of enterprises are behind in applying database security patches, while 74 percent of all Web application vulnerabilities – which are predominantly SQL Injection vulnerabilities – disclosed in 2008 did not even have an available patch by the end of 2008, according to IBM.

"You can't secure what you don't know. You need good mapping of your sensitive assets — both of your database instances and your sensitive data inside your databases."

Whereas most attention has previously been focused on securing network perimeters and client systems (firewalls, IDS/IPS, anti-virus, etc.), we are now entering a new phase where information security professionals are being tasked with ensuring that corporate databases are secure from breaches and unauthorized changes.

Here are 8 essential best practices that provide a holistic approach to both safeguarding databases and achieving compliance with key regulations such as SOX, PCI DSS, GLBA and data protection laws:

1. Discovery.

You can't secure what you don't know. You need to have a good mapping of your sensitive assets – both of your database instances and your sensitive data inside the databases. Plus, you should automate the discovery process since the location of sensitive data is constantly changing due to new or modified applications, mergers and acquisitions, etc.

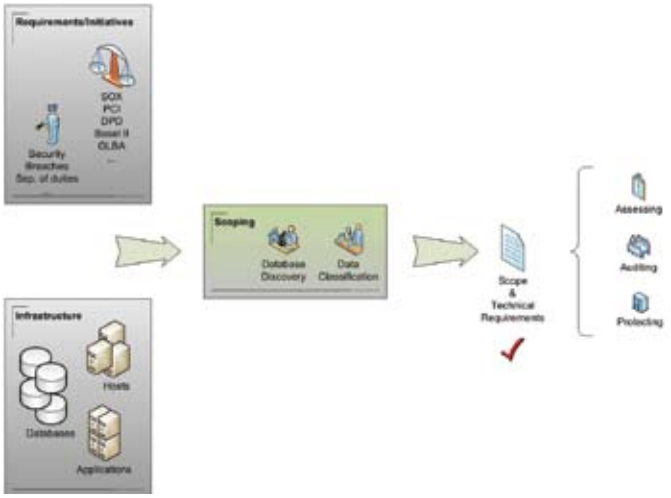


Figure 1: Using discovery tools to bootstrap an implementation. You need to map database instances as well as where your sensitive data is located.

1 "IBM Internet Security Systems X-Force® 2008 Trend & Risk Report," IBM Global Technology Services, Jan. 2009.
2 "Market Overview: Database Security," Forrester Research, Feb. 2009.

In an interesting twist, some discovery tools can also find malware placed in your database as a result of SQL injection attacks. In addition to exposing confidential information, SQL injection vulnerabilities allow attackers to embed other attacks inside the database that can then be used against visitors to the website.

2. Vulnerability and Configuration Assessment.

You need to assess the configuration of your databases to ensure they don't have security holes. This includes verifying both the way the database is installed on the operating system (for example, checking file privileges for database configuration files and executables) and configuration options within the database itself (such as how many failed logins will result in a locked account, or which privileges have been assigned to critical tables). Plus, you need to verify that you're not running database versions with known vulnerabilities.

Traditional network vulnerability scanners weren't designed for this because they don't have embedded knowledge about database structures and expected behavior, nor can they issue SQL queries (via credentialed access to the database) in order to reveal database configuration information.

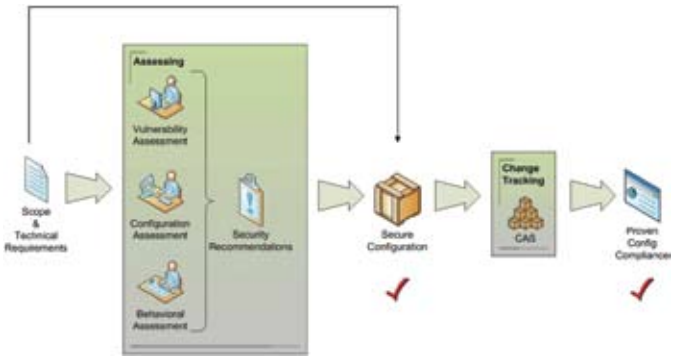


Figure 2: Vulnerability assessment and change tracking use case.

3. Hardening.

The result of a vulnerability assessment is often a set of specific recommendations. This is the first step in hardening the database. Other elements of hardening involve removing all functions and options that you do not use.

4. Change Auditing.

Once you've created a hardened configuration, you must continually track it to ensure that you don't digress from your "gold" (secure) configuration. You can do this with change auditing tools that compare snapshots of the configurations (at both the operating system level and at the database level) and immediately alert you whenever a change is made that could affect the security of the database.

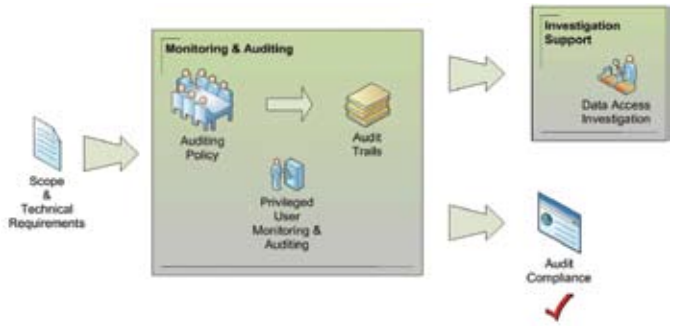


Figure 3: Use case for database activity monitoring (DAM) and auditing.

5. Database Activity Monitoring (DAM).

Real-time monitoring of database activity is key to limiting your exposure by immediately detecting intrusions and misuse. For example, DAM can alert on unusual access patterns indicating a SQL injection attack, unauthorized changes to financial data, elevation of account privileges, and configuration changes executed via SQL commands.

Monitoring privileged users is also a requirement for data governance regulations such as SOX and data privacy regulations such as PCI DSS. It's also important for detecting intrusions, since attacks will frequently result in the attacker gaining privileged user access (such as via credentials owned by your business applications).

DAM is also an essential element of vulnerability assessment, because it allows you to go beyond traditional static assessments to include dynamic assessments of "behavioral vulnerabilities" such as multiple users sharing privileged credentials or an excessive number of failed database logins.

"Not all data and not all users are created equally. You must authenticate users, ensure full accountability per user, and manage privileges to limit access to data."

Finally, some DAM technologies offer application-layer monitoring, allowing you to detect fraud conducted via multi-tier applications such as PeopleSoft, SAP and Oracle e-Business Suite, rather than via direct connections to the database.

6. Auditing.

Secure, non-repudiable audit trails must be generated and maintained for any database activities that impact security posture, data integrity or viewing sensitive data. In addition to being a key compliance requirement, having granular audit trails is also important for forensic investigations.

Most organizations currently employ some form of manual auditing utilizing traditional native database logging capabilities. However, these approaches are often found to be lacking because of their complexity and high operational costs due to manual efforts. Other disadvantages include high performance overhead, lack of separation of duties (since DBAs can easily tamper with the contents of database logs, thereby affecting non-repudiation) and the need to purchase and manage large amounts of storage capacity to handle massive amounts of unfiltered transaction information.

Fortunately, a new class of DAM solutions are now available that provide granular, DBMS-independent auditing with minimal impact on performance, while reducing operational costs via automation, centralized cross-DBMS policies and audit repositories, filtering and compression.

7. Authentication, Access Control and Entitlement Management.

Not all data and not all users are created equally. You must authenticate users, ensure full accountability per user, and manage privileges to limit access to data. And you should enforce these privileges – even for the most privileged database users. You also need to periodically review entitlement reports (also called User Right Attestation reports) as part of a formal audit process.

8. Encryption.

Use encryption to render sensitive data unreadable, so that an attacker cannot gain unauthorized access to data from outside the database. This includes both encryption of data-in-transit, so that an attacker cannot eavesdrop at the networking layer and gain access to the data when it is sent to the database client, as well as encryption of data-at-rest, so that an attacker cannot extract the data even with access to the media files.

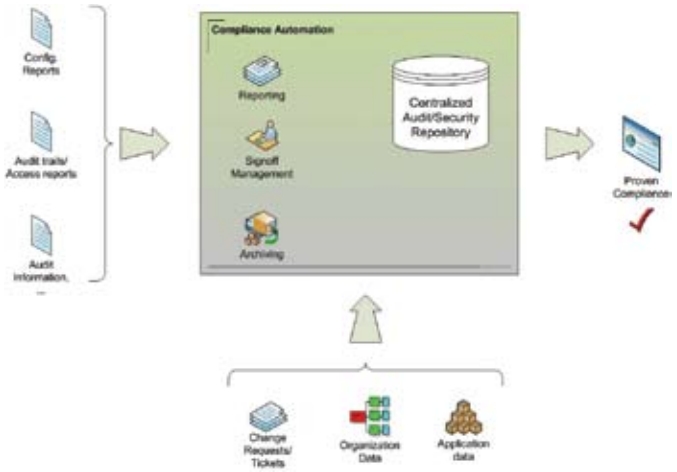


Figure 4: Managing the entire compliance lifecycle.

8 Steps to Database Security

1. Discovery
2. Vulnerability & Configuration Assessment
3. Hardening
4. Change Auditing
5. Database Activity Monitoring (DAM)
6. Auditing
7. Authentication, Access Control & Entitlement Management
8. Encryption

About the Author

Dr. Ron Ben Natan commands more than 20 years of experience developing enterprise applications and security technology for blue-chip companies such as Merrill Lynch, J.P. Morgan, Intel and AT&T Bell Laboratories. Ron also served as a consultant in data security and distributed systems for Phillip Morris, Miller Beer, HSBC, HP, Applied Materials and the Swiss Armed Forces.

An IBM GOLD consultant with a Ph.D. in computer science, Ron is an expert on distributed application environments, application security, and database security. He has authored 12 patents as well as 12 technical books including *Implementing Database Security and Auditing* (Elsevier Digital Press), the standard text in the field, and Ron's newest book *HOWTO Secure and Audit Oracle 10g and 11g* (CRC Press) published in 2009.

About IBM InfoSphere Guardium

InfoSphere Guardium is the most widely-used solution for preventing information leaks from the data center and ensuring the integrity of enterprise data. It is installed in more than 400 customers worldwide, including 5 of the top 5 global banks; 4 of the top 6 insurers; top government agencies; 2 of the top 3 retailers; 20 of the world's top telcos; 2 of the world's favorite beverage brands; the most recognized name in PCs; a top 3 auto maker; a top 3 aerospace company; and a leading supplier of business intelligence software. InfoSphere Guardium was the first solution to address the core data security gap by providing a scalable, cross-DBMS enterprise platform that both protects databases in real-time and automates the entire compliance auditing process.

Guardium is part of IBM InfoSphere; an integrated platform for defining, integrating, protecting and managing trusted information across your systems. The InfoSphere Platform provides all the foundational building blocks of trusted information, including data integration, data warehousing, master data management, and information governance, all integrated around a core of shared metadata and models. The portfolio is modular, allowing you to start anywhere, and mix and match InfoSphere software building blocks with components from other vendors, or choose to deploy multiple building blocks together for increased acceleration and value. The InfoSphere Platform provides an enterprise-class foundation for information-intensive projects, providing the performance, scalability, reliability and acceleration needed to simplify difficult challenges and deliver trusted information to your business faster.

IBM Corporation
Route 100
Somers, NY 10589

Produced in the United States of America
May 2010

Please Recycle

InfoSphere®
software

IMW14277-CAEN-01