Solution Brief

McAfee®
An Intel Company

Not All Database Security Solutions Are Created Equal

Compare solutions from different vendors

Databases are the number one target of cybercriminals and disgruntled insiders. With the recent rash of breaches, you may have already realized that traditional perimeter and network security, as well as built-in database security measures, offer only very limited protection when it comes to securing the organization's most sensitive data, which is often stored in databases. That's why compliance officers as well as auditors are taking a much closer look at database security and compliance. It is also why four main database security vendors have entered the market. This document highlights key database security capabilities and provides an objective, apples-to-apples comparison of the leading database security solutions.

What Your Database Security Solution Should Do

- *Protect all your databases across all threat vectors in real time*—Partial protection or after-the-fact notifications are of little value if your database has already been compromised. Make certain that you protect "all doors and windows" (not only what the vendor can support) and that you receive real-time, actionable insights.
- *Establish and verify a security baseline across all your databases*—Does the solution provide comprehensive vulnerability detection that spans all your database platforms? How often is the scan list updated by the vendor in response to new threats? Is the scan library based on a theoretical framework (for example, database vendor recommendations and industry guidelines), or is it based on real-world security know-how? Can it integrate with your organization's current IT security landscape: security information event management (SIEM), McAfee® ePolicy Orchestrator® (McAfee ePO™) software, and database administration management (DAM) system?
- *Provide detailed reporting and continuous compliance*—The ability to quickly validate and document compliance will become even more important going forward. Integrated compliance reporting through a central management platform is a must.
- *Easily deploy across complex and heterogeneous IT environments (including virtual and cloud)*—Today's databases are a hybrid combination of dedicated and virtualized environments that span multiple platforms. Your database security solution must protect all of them.
- *Quickly and easily scale to meet your growth and performance needs*—How quickly can the solution be deployed? What resources are required to deploy and manage it? Does the solution require hardware appliances? If so, how many must be added, and how will they be managed? What are the maintenance implications?
- *Help ensure segregation of duties for privileged users*—SOX, PCI-DSS, HITECH, and numerous global privacy regulations now require that your organization enforce and monitor segregation of duty access to sensitive databases.

Databases: The Top Regulatory Compliance Challenge
In January 2012, Evalueserve surveyed 438 IT decision makers, administrators, consultants, and security analysts worldwide. Respondents listed databases as their most challenging regulatory compliance area.

Databases are the leading IT security blind spot
In April 2012, Verizon Business released its annual data breach survey (covering more than 800 security breaches), which found that database breaches accounted for 95% of all records breached.

> *"We were able to get more value out of McAfee's DB [McAfee database] security product in two weeks than we got from our older DAM product in over a year."*
>
> —Director of IT Security
> Financial services company

What Your Database Security Solution Should Not Do

- *Create an additional security management silo*—Who has time to learn and manage multiple point products or manually sort through database log files? Disjointed security products that lack an integrated security management console result in time-consuming, reactive, and ineffective database protection and often involve lengthy deployment and configuration. Time-consuming, resource-intensive, and operationally disruptive deployment and integration engagements delay protection and may result in ongoing maintenance commitments.
- *Degrade application/database performance*—A database security solution cannot slow down business-critical database services. Solutions that force you to compromise and disable certain features so as to reduce the database performance impact or reduce your network load can be counterproductive.
- *Require substantial time and effort for setup and management*—This especially a problem if this occurs on an ongoing basis.
- *Based on a business-model that is complex*—Such solutions can be difficult to track and control, may introduce risk of future licensing surprises (for example, they cannot be properly scoped upfront), may require a repurchase of the solution every few years (for example, appliance hardware refresh cycle), and could open you up to potential enforcement and litigation risks.

How McAfee Database Security Solutions Stack Up Against the Competition

Take a closer look at the key functional capabilities you need and how the McAfee Database Security solution compares to the competition in each of the following areas.

Database vulnerability management

Most vulnerability assessment products aren't comprehensive and intelligent enough to thoroughly test database systems, putting your most sensitive and valuable data at risk. Compulsory for any database security solution is the ability to discover any and all databases on your network, identify the ones that contain sensitive data (credit card numbers, Social Security numbers, and passwords), determine if the latest patches have been applied, and perform an extensive (and regularly updated) comprehensive testing to identify security weaknesses. Used properly, a database vulnerability management solution can help you establish a security baseline across a large number of sensitive databases and periodically monitor databases to highlight any drifts from the approved baseline.

Vulnerability Testing

Vulnerability Testing	IBM InfoSphere Guardium	Imperva SecureSphere DAM	Application Security AppDetective Pro/DB Protect	McAfee Database Security Solution
Number of Vulnerability Tests	1,000 vulnerability tests, mostly based on vendor recommendations and industry standards.	2,000 vulnerability tests, mostly based on vendor recommendations and industry standards.	2,000 vulnerability tests.	4,700 vulnerability tests and checks (including CIS and STIG scans).
Frequency of Scan Library Update	Infrequently	Infrequently	A few times a year.	Every four weeks on average.
Fast Weak Password Scanner	Slow	Slow	Slow	Very fast scanning algorithm (more than one million combinations per second).
McAfee ePO Software Integration	No	No	No	Yes—It improves visibility and automates management, vulnerability analysis, and reporting in a single console.

Database activity monitoring (DAM)

Perimeter and network protection measures and basic security measures built into databases do not provide adequate security to sensitive databases. They don't protect you from today's sophisticated hackers and malicious insiders. An effective database activity monitoring solution must be easy to manage and provide comprehensive protection against modern threats and be able to not only alert, but also stop attacks before they can cause damage.

Database Performance Impact of Activity Monitoring

Your database and the networks that provide access to them must remain available and responsive. In addition, you need a database security solution that can provide real-time, actionable insights, not just after-the-fact forensics. The McAfee Database Security solution provides a clear competitive advantage in these areas:

Performance

Performance	IBM InfoSphere Guardium	Imperva SecureSphere	Oracle DataWall	McAfee Database Security Solution
Autonomous Agents (minimize network traffic and server I/O consumption)	No—Sensors must send traffic over the network to a collector appliance for analysis, increasing both server and network load. Agents cache traffic to local disk consuming server I/O and impacting database performance. Blocking requires proxy agents (S-Gate) that introduce latency.	No—Database host agents must send traffic over the network to the SecureSphere appliance(s) for analysis, increasing network load.	No—Database host agents must send traffic over the network to the SecureSphere appliance(s) for analysis, increasing network load.	Yes—Minimal performance impact: is less than 5% of a single host core CPU per monitored instance, less than 100 MB of RAM. No I/O consumption. Sensors do not introduce latency.
Frequency of Scan Library Update	Disruptive—Requires database/ server shutdown for initial installation and subsequent agent upgrades.	Requires database/server shutdown for initial installation and subsequent agent upgrades.	Requires database/server shutdown for initial installation and subsequent agent upgrades.	Transparent—Agent installation and subsequent upgrade does-not involve server or database shutdown.
Agent Architecture	Intrusive—Agents operate at the kernel level and can affect database and server performance. Blocking agents (S-Gate) installed as proxies introducing latency.	Intrusive—Agents operate at the kernel level and can affect database and server performance.	Intrusive—Agents operate at the kernel level and can affect database and server performance.	Non-intrusive—Sensors not installed at the kernel level and therefore cannot interfere with database/server performance.

Database Activity Monitoring Implementation and Capabilities

Database Activity Monitoring	IBM InfoSphere Guardium	Imperva SecureSphere DAM	Oracle DataWall (formerly Secerno)	Application Security DB-Protect	McAfee Database Security Solution
Underlying Monitoring Technology	SQL sniffing via network appliances and/or local host forwarding agents. Limited visibility and easy to evade (relies only on the actual text of the SQL command).	SQL sniffing via network appliances and local host forwarding agents. Limited visibility and easy to evade (relies only on the actual text of the SQL command).	SQL sniffing via network appliances and local host forwarding agents. Limited visibility and easy to evade (relies only on the actual text of the SQL command).	SQL sniffing via forwarding agents. Limited visibility and easy to evade (relies only on the actual text of the SQL command).	Monitors by analyzing the database shared memory, providing much more visibility into threats (able to monitor transactions that originate inside the database itself and able to understand how the database interpreted obfuscated SQL payloads).
Autonomous versus Console-Dependent Analysis and Blocking	Dependent—Database-server agent(s) forward all database traffic back to one or more appliances (collectors) for actual analysis. Requires management appliance to aggregate and manage the collectors.	Dependent—Appliance monitors network traffic (requires SPAN/TAP port), and database-server agent(s) forward(s) all local database traffic back to the network appliance(s) for analysis.	Dependent—Appliances monitor network traffic (requires SPAN/TAP port), and database-server agent(s) forward(s) all local database traffic back to the network appliance(s) for analysis.	Dependent—Database server agent(s) forward(s) all database traffic back to appliance(s) for analysis.	Autonomous—Software-only solution utilizes host-based non-intrusive and lightweight autonomous agents (sensors) that monitor the database memory. The autonomous sensors perform the monitoring locally and do not need to forward the full database traffic to an external appliance for analysis. Only relevant events are forwarded to the management console. Sensors do not operate at the kernel level and do not cache traffic to the server hard disk.
Smart, Comprehensive Agent Technology	No—Intrusive (kernel-level) agents that forward database traffic to an external collector for analysis. Caches traffic to local disk (degrading database performance). S-Gate (blocking) agents act as proxies, delaying transaction execution. Lacks visibility into intra-database activity (dynamic stored procedures, triggers, views, obfuscated payloads, and more). Database and host crashes and restarts are not uncommon.	No—Kernel-based agent involves DBMS instrumentation and degrades performance. Agent monitors only the local host traffic but doesn't provide visibility into intra-database activity.	No	No	Yes—Intelligent, autonomous agent monitors database memory and provides full visibility into all database activity, including transactions originating from inside the database itself (intra-database traffic). This read-only process at the operating system level does not require any database or host downtime, generate any latency, or consume any input/output.
User-Based Application Monitoring for Multitier Environments	Yes	Partial—Based on correlating event information from WAF logs and DAM logs. Accuracy of matching is not guaranteed and deteriorates rapidly as traffic volume grows.	No	No	Yes (accurate)—McAfee iDentifier module captures end-user identity with 100% accuracy regardless of traffic volume, providing full visibility and reporting into who is doing what in the database.
Monitors at the Database Object Level and Obfuscated Payloads	No—Cannot monitor at the database object level (limited to only seeing the text of the SQL command) and blind obfuscated SQL payloads that can be used by hackers/insiders to easily bypass monitoring.	No—Cannot monitor at the database object level (limited to only seeing the text of the SQL command) and blind obfuscated SQL payloads that can be used by hackers/insiders to easily bypass monitoring.	No—Cannot monitor at the database object level (limited to only seeing the text of the SQL command) and blind obfuscated SQL payloads that can be used by hackers/insiders to easily bypass monitoring.	No—Cannot monitor at the database object level (limited to only seeing the text of the SQL command) and blind obfuscated SQL payloads that can be used by hackers/insiders to easily bypass monitoring.	Yes—McAfee memory-based sensors can see the actual database object being accessed (even if it is not mentioned in the SQL command text). Allows seamless monitoring of all database traffic, including obfuscated payloads (which are visible to the sensor "in the clear" in the database memory).

Database Activity Monitoring Implementation and Capabilities

Database Activity Monitoring	IBM InfoSphere Guardium	Imperva SecureSphere DAM	Oracle DataWall (formerly Secerno)	Application Security DB-Protect	McAfee Database Security Solution
Effective Prevention of Unauthorized Local Transactions	Partial (very intrusive and rarely used)—Can miss malicious or unauthorized activity as SQL traffic is sent back to the management appliance for analysis. By the time a statement is defined as rogue, it is too late to be blocked. Additionally, blocking requires use of a different agent (S-GATE), which acts as a proxy, adding latency and consuming I/O (caches traffic to disk). It can be easily bypassed by accessing the original database port.	Partial—Network blocking only (no local host traffic blocking). Network appliance must be in-line to block network threats, introducing a single point of failure in the critical path. Agents cannot block local traffic at all.	Partial—Network blocking only (no local host traffic blocking). Network appliance must be in-line to block network threats, introducing a single point of failure in the critical path. Agents cannot block local traffic at all.	No	Yes—McAfee can effectively block many types of malicious or unauthorized activity in real time. Because the sensor monitors transactions in memory, operates autonomously and resides on the host system, it can intervene and terminate connections immediately.
Establishes Segregation of Duties	Partial—Due to the limitations of SQL sniffing technology, privileged insiders and sophisticated hackers can evade monitoring/detection simply by using obfuscated SQL payloads, dynamic views, and stored procedures.	Partial—Due to the limitations of SQL sniffing technology, privileged insiders and sophisticated hackers can evade monitoring/detection simply by using obfuscated SQL payloads, dynamic views, and stored procedures.	Partial—Due to the limitations of SQL sniffing technology, privileged insiders and sophisticated hackers can evade monitoring/detection simply by using obfuscated SQL payloads, dynamic views, and stored procedures.	Partial—Due to the limitations of SQL sniffing technology, privileged insiders and sophisticated hackers can evade monitoring/detection simply by using obfuscated SQL payloads, dynamic views, and stored procedures.	Yes—Database memory monitoring technology sees all database transactions, including access originating inside the databases. Able to detect the actual objects accessed by the database and monitor obfuscated SQL payloads (which are monitored in the clear in the database memory). Establishes strict separation of duties.
Script signing	No	No	No	No	Yes—The ability to digitally sign database scripts ensures that they are not modified prior to execution (patent pending).
Ability to identify SUDU users	No	No	No	No	Yes

Ease of use and deployment

Complex security products require more training and additional consulting and integration costs, which should be taken into account when calculating the total cost of ownership of a solution. What's more, their complexity often results in partial use of product features, resulting in reduced database protection. Solutions that generate too much data or hard-to-decipher security data in unusable formats complicate the database security challenge.

Ease of Deployment and Use

Ease of Deployment and Use	IBM InfoSphere Guardium	Imperva SecureSphere	Application Security	McAfee Database Security Solution
Easy to Install	No—Routinely requires weeks of professional services to deploy and configure.	No—Routinely requires weeks of professional services to deploy and configure.	No—Routinely requires weeks of professional services to deploy and configure.	Yes—Software-only solution, easy to install and configure. Does not require network setup changes, SPAN/TAP port provisioning. Simple installations completed in hours.
Agents Installation and Upgrade Process	Intrusive—Often requires database/server restart.	Intrusive—Often requires database/server restart.	Intrusive—Often requires database/server restart.	Non-intrusive—Installation and upgrades of the sensors do not require any database or server restart.
Flexible Deployment in Different Network Topologies/ Distributed Environments	No—Requires one or more collector appliances per location.	Yes	Yes	Yes—Software only and network agnostic. Topology doesn't impact ease of use or management. Smart sensors run in memory on each database. Thousands of sensors monitoring databases in multiple geographies can all be managed from a single MDAM management console.
Effective in Cloud and Virtualized Environments	No—All traffic must be sent to central server for evaluation; dynamic infrastructures create out-of-date configurations.	No—All traffic must be sent to central server for evaluation; dynamic infrastructures create out-of-date configurations.	No—Some tools (such as database firewall) require appliance installation.	Yes—Sensor-based architecture performs perfectly in distributed models, including virtual machines and cloud-based architectures.
McAfee ePO Software Integration	No	No	No	Yes

Business Model Differences

Ease of Deployment and Use	IBM InfoSphere Guardium	Imperva SecureSphere	Oracle DataWall	McAfee Database Security Solution
Total Cost of Ownership	Appliance-based model requires costly appliance upgrades every three to five years. Large/complex environments require many appliances (collectors).	Appliance-based model requires costly appliance upgrades every three to five years. Large/ complex environments require many appliances (collectors). Requires TAP/SPAN ports, which might entail additional hardware costs. Appliances may require unexpected costly upgrades once traffic volume exceeds the appliance rated capacity.	Appliance-based model requires costly appliance upgrades every three to five years. Large/complex environments require many appliances (collectors). Requires TAP/SPAN ports, which might entail additional hardware costs. Appliances might require costly upgrades once traffic volume exceeds the appliance rated capacity.	No appliances, no hardware upgrade cycle. Simple deployment reduces total cost of ownership. No additional costs as database traffic grows. No additional costs associated with TAP/SPAN ports (not required).
Simple, Predictable, and Scalable Business Model	No—Complex model (PVU is dependent on CPU core count and CPU model factors and hundreds of SKUs). High risk of inadvertent licensing compliance violations due to routine server upgrades. Dozens of modules sold as add-ons at extra cost.	No—Traffic volume-based business model, often leads to additional unexpected license costs as database traffic volume grows. Database traffic blocking sold as an add-on to the basic monitoring capability.	No—Traffic volume-based business model often leads to additional unexpected license costs as database traffic volume grows.	Yes—Simple and scalable model based on the number of database instances monitored. No additional costs. Most functionality is included out-of-the-box and does not require additional licensing.

For more information on the unique and powerful McAfee approach to helping you secure your business-critical databases, visit www.mcafee.com/dbsecurity.
Follow us on Twitter: @McAfeeBusiness.

McAfee
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com