McAfee
An Intel Company

# PCI DSS Compliance for Databases

## Comply fully and reduce database security risk

**_SC Magazine_ 2012 Best Database Security Solution**
McAfee Database Activity Monitoring received *SC Magazine's* 2012 Gold Award for Best Database Security Solution.

SC MAGAZINE AWARDS 2012 WINNER
Honored in the U.S.

### Benefits of McAfee Database Activity Monitoring

- Maximizes visibility and protection from all sources of attacks
- Monitors external threats, privileged insiders, and sophisticated threats from within the database
- Provides alerts and even terminates unauthorized or suspicious activities before they can cause damage
- Includes virtual patching to protect databases from threats even before installing vendor-released patches
- Can be implemented on databases in under an hour

Recent surveys of IT managers have revealed two commonly held beliefs: database regulations are the most challenging to comply with, and, of all regulatory standards, the Payment Card Industry Data Security Standard (PCI DSS) is the toughest.[1] These findings should come as no surprise. After all, anyone who processes, stores, or transmits credit card information must comply with PCI DSS by maintaining a secure environment, and, these days, that's not easy. However, McAfee® database security is made to order for complying with PCI DSS. What's more, it enables organizations to move beyond mere compliance—all the way up to comprehensive protection of systems and data.

### What PCI DSS Requires

PCI DSS compliance is an ongoing process that, according to the PCI Security Standards Council, involves three basic steps:

- *Assess*—Identify cardholder data and associated databases, as well as potential threats and vulnerabilities that could expose cardholder data
- *Remediate*—Block known threats and fix vulnerabilities by establishing which systems are adequately protected and implement security solutions to protect systems that are not protected
- *Report*—Compile and submit required remediation validation records (if applicable) and submit compliance reports to internal auditors or to the appropriate bank or card brands

McAfee database security covers all the bases. It enables you to thoroughly assess the strength of your security environment by providing visibility into where databases are located, which ones contain sensitive information, and the extent to which they are protected. With this knowledge, you can remediate vulnerabilities and apply safeguards against threats known and unknown. Reporting is simple because McAfee database security provides templates and makes the necessary information available at all times.

### Key Building Blocks

To maintain the secure environment that the PCI DSS standard requires, you need a comprehensive, multifaceted solution. While some solution components may vary depending on the size and type of the individual enterprise, there are three that provide an efficient, cost-effective security foundation for virtually any organization that must comply with PCI DSS:

- McAfee Database Activity Monitoring
- McAfee Database Vulnerability Manager
- McAfee® ePolicy Orchestrator® (McAfee ePO™) software

### McAfee Database Activity Monitoring

McAfee Database Activity Monitoring protects your most valuable and sensitive data from external threats originating outside the network perimeter; from local users logged in to the server itself, including privileged users; and even from attacks that originate within the database using stored procedures or triggers. This software-only solution can be installed in less than an hour to monitor activity on each database server and prevent intrusion in real time, even when running in virtualized or cloud computing environments. It uses memory-based sensors to detect attacks and stop breaches

before they cause damage. Alerts are sent directly to the monitoring dashboard with full details of the policy violation for remediation purposes. The software can be configured to automatically terminate suspicious sessions and quarantine malicious users, allowing time for the security team to investigate the intrusion. McAfee Database Activity Monitoring also comes with a PCI DSS compliance monitoring template that shortens the time it takes to become compliant.

### Virtual patching protects from known exploits and many zero-day threats

There are times when, try as you might, you simply can't do everything to the letter. Installing vendor patches *immediately*, for instance, is rarely an option. Replacing multiple, no-longer-supported legacy databases in one fell swoop isn't practical either. For these reasons, McAfee Database Activity Monitoring includes McAfee Virtual Patching for Databases (vPatch), which updates for newly discovered vulnerabilities. Not only does McAfee Database Activity Monitoring detect attacks attempting to exploit known vulnerabilities in real time, with virtual patching, you can implement an interim layer of protection until a patch is released by the database vendor and can be applied, or until a legacy database is replaced. This way, you can protect sensitive data without database downtime. It's like an intrusion prevention system for databases—so you can tell auditors that you have adequate safeguards in place.

As new vulnerabilities are discovered, updates with new virtual patch rules are released by McAfee and can be automatically distributed to all covered databases through a centralized management console. Not only does this solution save time, it supports a proactive patching strategy, allowing you to schedule database patch deployment within your preferred timeframe. It protects against more than 450 vulnerabilities.

### A substitute for data encryption

McAfee Database Activity Monitoring can be used as a compensating control for databases that don't support payment card data encryption. The object-level McAfee Database Activity Monitoring solution prevents access to payment card data tables from users or applications that aren't on approved lists. Moreover, it lets you see every access episode to any tables that contain sensitive data. So, you can tell your auditors that McAfee Database Activity Monitoring serves the same purpose as encryption—keeping prying eyes and potentially harmful pieces of code from accessing sensitive data.

#### Benefits of McAfee Vulnerability Manager for Databases

- Automatically discovers databases on the network and determines if the latest patches have been applied
- Tests for weak passwords, default accounts, and other weaknesses
- Provides "fix scripts" for high-priority vulnerabilities
- Conducts more than 4,500 vulnerability checks against leading database systems
- Provides out-of-the-box PCI DSS compliance reports

## McAfee Vulnerability Manager for Databases

The PCI DSS standard requires organizations to establish a process that identifies newly discovered security vulnerabilities. First, of course, you have to locate those vulnerabilities, and that's where McAfee Vulnerability Manager for Databases comes in. It locates your databases and any tables containing payment card data and other sensitive information; determines if the latest patches have been applied; and tests for vulnerabilities such as weak passwords, default accounts, and other common weaknesses. Then it classifies threats into distinct priority levels and provides "fix scripts" for the highest-priority vulnerabilities. McAfee Vulnerability Manager for Databases conducts more than 4,500 vulnerability checks against leading database systems, including Oracle, SQL Server, Sybase, DB2, PostgreSQL, and MySQL. It also provides out-of-the-box regulatory compliance reports and custom reports for PCI DSS regulations.

#### Benefits of McAfee ePolicy Orchestrator Software

- Provides centralized reporting and summary information for all your databases from a consolidated dashboard
- McAfee Database Activity Monitoring and McAfee Vulnerability Manager for Databases plug in to McAfee ePO software for comprehensive views of security status and threats
- Extensible security management platform integrates with and leverages your existing IT infrastructure

## McAfee ePolicy Orchestrator Software

Both McAfee Database Activity Monitoring and McAfee Vulnerability Manager for Databases integrate with McAfee ePO software. As a result, you can obtain end-to-end visibility and centralized reporting and summary information for thousands of databases from a single dashboard. With McAfee ePO software, you can centralize your PCI DSS compliance processes and all of your IT security. It doesn't get any easier.

## Learn More

Discover how to efficiently and cost effectively comply with PCI DSS while implementing a comprehensive database security solution. Visit www.mcafee.com/dbsecurity, or contact your local McAfee representative or reseller.

[1] *Risk and Compliance Outlook 2012*, Evalueserve, Inc.

McAfee
An Intel Company

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


47000brf_pci-dss_0712_fnl_ETMG