Solution Brief

Database-Friendly Security

Safeguard data. Preserve performance.

All database security products are not created equal. Many do the job but are a drag on database performance. Others add administrative complexity. And a few even insert points of failure. McAfee® Database Security stands out from the crowd because it addresses all of these issues.

Businesses run on databases. No one understands this better than database administrators. With today's onslaught of database security attacks and breaches, protecting databases has quickly become the focus of security teams, compliance officers, and executive staff. As a result, the role of DBAs is more critical to the organization than ever before—and more complex. DBAs must work with their security and compliance peers to protect databases and maintain compliance. However, without a dedicated database security and patching solution, this process can consume a database administrator's time and resources and jeopardize delivery on performance and uptime service-level agreements.

Automate Protection

McAfee Database Security offers real-time protection for business-critical databases from all vectors and types of threats: external, internal, and even intra-database exploits. This software-based database security solution is an efficient, affordable, and easily deployable way to protect databases while preserving database performance and helping to ensure continuous business operations.

McAfee Database Security comprises several industry-leading, tightly integrated modules to deliver comprehensive protection that goes far beyond native, easily bypassed database management system (DBMS) security capabilities. McAfee Database Security allows you to customize and tune database protection, automating the processes of database discovery, vulnerability assessment, real-time monitoring, and security policy enforcement. Here's how it works:

- McAfee Vulnerability Manager for Databases automatically discovers all databases across your environment, helps you assess security weaknesses, and generates actionable reports on how to harden your databases against them
- McAfee Virtual Patching for Databases protects databases against known vulnerabilities by detecting and preventing attempted attacks and intrusions without requiring database downtime or application testing or modification
- McAfee Database Activity Monitoring provides visibility into all database activity—including malicious back doors—and protects the database in real time from threats and unauthorized activity

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.

For companies seeking enterprise-wide security management, visibility, and reporting, the entire McAfee Database Security solution is tightly integrated with McAfee® ePolicy Orchestrator® (McAfee ePO™) software—the industry's most advanced and scalable security management platform.

Challenge: The ongoing race to close the security patch vulnerability window

From the minute a database vendor releases an update to patch a vulnerability, the clock starts ticking. Not only does this release inform customers of the security risk, it makes hackers aware of their opportunity to exploit the database—dramatically increasing the likelihood of an attack. This "window of vulnerability" continues until the security patch is applied to each database.

In an ideal world, patches would be applied as soon as they are issued. However, in the real world, that's a significant hardship. Large companies often have 1,000 or more databases that require patching. Assuming the database vendor issues patches on a quarterly basis, applying these updates can require four person-hours per database to patch—that's 4,000 hours or more of database patching. And since patching is an update to the DBMS kernel, this arduous process requires bringing down the databases and rigorously testing applications against these changes.

It's easy to understand why so many databases are running in an unpatched, vulnerable state.

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. The inability to apply security patches in a timely manner is a major reason why.

McAfee Virtual Patching: A Practical Compensating Control

McAfee Virtual Patching for Databases reduces the risk presented by unpatched vulnerabilities by detecting, and preventing attempted attacks and intrusions in real time. What's more, it provides this protection without requiring database downtime or application testing. This innovative virtual patching solution also helps you continue to protect databases running older DBMS versions that are no longer supported by the vendor, adding to the useful life of legacy databases and saving your organization time and money.

The McAfee Virtual Patching service is continuously updated by the McAfee security team. Virtual patches are seamlessly distributed and applied approximately once per month. In addition, once the DBMS vendor releases a patch update, McAfee Virtual Patching normally provides protection within 48 to 72 hours following a patch release. The solution addresses more than 500 vulnerabilities (as of June 2012).

Not only does this solution save time, it serves as a compensating control until your organization is ready to deploy the vendor patches. Compliance auditors recognize McAfee Virtual Patching as valid compensating control that allows you to maintain business continuity without sacrificing regulatory compliance.

Deploying the vendor patches is always the recommended policy. However, if your organization runs databases that cannot be taken offline for patching, or if you have a large database population that's creating patch deployment delays, virtual patching may be the answer.

McAfee Virtual Patching Advantages

- Protect databases from threats even before installing vendor-released patches
- Keep production databases online, thanks to non-intrusive software design
- Protect databases seamlessly with automatic distribution of ongoing updates
- Facilitate compliance with PCI DSS, HIPAA, and other standards
- Protect both current and end-of-life databases

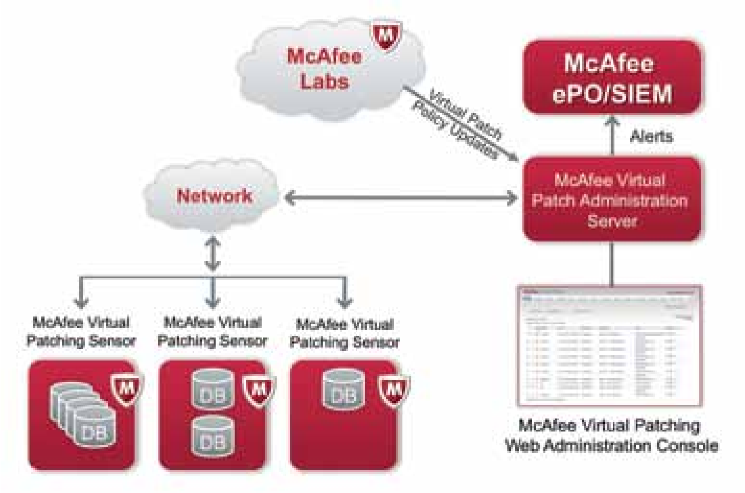
McAfee Labs
McAfee ePO/SIEM
Virtual Patch Policy Updates
Alerts
Network
McAfee Virtual Patch Administration Server
McAfee Virtual Patching Sensor
McAfee Virtual Patching Sensor
McAfee Virtual Patching Sensor
DB
DB
DB
DB
McAfee Virtual Patching Web Administration Console

Figure 1. The McAfee security team routinely researches and monitors database security issues. When an issue is discovered or a patch is released by a database vendor, McAfee deploys the virtual patching rules to a central server. Protected databases poll the McAfee Virtual Patching servers and deploy protection automatically or according to a predefined schedule. Once a security update is downloaded, it is pushed immediately to relevant sensors.

> *"We knew we needed to do more to secure our databases. We chose Hedgehog [McAfee Database Activity Monitoring], as we could install it quickly and easily, and, unlike network-based solutions, it protects us against all types of attacks."*
>
> —Cameron Capewell
> Database Administrator
> University of Bristol

Challenge: Maintain database integrity, performance, and uptime

There's a reason why many DBAs view database security solutions with a healthy dose of skepticism. Many solutions add performance overhead to the database and introduce a single point of failure to database systems. In stark contrast, McAfee Database Security components are based on a non-intrusive design that causes minimal performance impact.

> *"The top tools being implemented to manage risk and achieve compliance are database activity monitoring (73 percent), followed by monitoring of configuration changes (63 percent)."*
>
> *—Evalueserve 2012*
> *Risk and Compliance Outlook*
> January 2012

Award-Winning Database Monitoring with Minimal Overhead

McAfee Database Activity Monitoring monitors all database activity in real-time based on pre-defined or custom rules and policies. It issues alerts on suspicious activity and prevents intrusion by terminating sessions that violate security policy, while providing a reliable audit trail of all database user activity.

McAfee Database Activity Monitoring makes use of small footprint software agents that are installed on database host servers at the operating system level, and these agents monitor all database activity. The design is non-intrusive, easy to install, and consumes only small amounts of CPU resources (less than 5 percent of a single core/CPU per monitored instance—even on multiple processor machines). The sensors communicate with the McAfee Database Activity server, which generates alerts in accordance with its defined rules.

This affordable, software-only solution can be deployed in less than one hour without the need for special hardware or additional servers. It scales cost effectively to address your growing database monitoring needs, and the memory-based sensor implementation is ideal for both virtualized and cloud environments.

Challenge: Assessing the risk of your most sensitive data

Detecting vulnerabilities before they are exploited is the goal of any database security strategy. That's where effective vulnerability assessment comes in. By assessing these vulnerabilities, you can pinpoint and prioritize risk remediation, protecting your most valuable data assets while avoiding a "when-in-doubt-patch" approach.

McAfee Vulnerability Manager for Databases

McAfee Vulnerability Manager for Databases helps identify weaknesses, threats, and configuration and security holes in databases that can be exploited by intruders and hackers to gain access to database resources. It automatically discovers databases on your network, determines if the latest patches have been applied, and tests for common vulnerabilities, such as weak passwords, default accounts, and more. McAfee Vulnerability Manager for Databases conducts more than 4,500 individual vulnerability checks on Oracle, Microsoft SQL Server, IBM DB2, Sybase, MySQL, Postgres SQL, and SQL Azure databases.

When coupled with McAfee Database Activity Monitoring, McAfee Vulnerability Manager streamlines security practices—not only for IT security and compliance teams, but also for database administrators.

Keep Databases Safe and Available. Learn More.

At McAfee, we realize your databases store your most critical business assets. They must be available around the clock to power your business. And, just as your databases don't take a day off, neither do we. Our team of database security experts remains relentlessly focused on keeping your sensitive information safe and available, while helping your company ensure compliance with internal policies and industry regulations.

All three McAfee database security modules are available for a complimentary trial to qualified prospects. For more detailed information on how the McAfee Database Security solution can help you protect your databases, visit www.mcafee.com/dbsecurity, or contact your local McAfee representative or reseller.

Follow us on Twitter: @McAfee_DBSecure

McAfee
An Intel Company

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

McAfee, the McAfee logo, ePolicy Orchestrator, and McAfee ePO are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other marks and brands may be claimed as the property of others. The product plans, specifications and descriptions herein are provided for information only and subject to change without notice, and are provided without warranty of any kind, express or implied.
Copyright © 2012 McAfee, Inc.