White Paper

Hardening Databases

Address database security and compliance without sacrificing availability or performance

Table of Contents

Databases contain your company's most valuable information assets. They are also the number one target of cybercriminals. And yet, in many organizations, databases are poorly protected and frequently flagged for compliance violations. Common sense dictates that databases can and must be secured as well as or better than any systems in the enterprise. So, why does securing databases pose such a formidable challenge to DBAs and IT security staff, and what can be done to improve the process? This paper takes a look at the security, compliance, and operational challenges facing IT teams and explains how the McAfee can help resolve today's most pressing database security issues.

Introduction

The process for securing databases and maintaining compliance can be fragmented, resource-intensive, and costly. All too often, it requires a growing list of disjointed point products, arduous patching processes, and operational issues involving the availability and performance of databases—business-critical systems that are difficult to take offline for necessary security maintenance. Regardless of logistical challenges, your databases must be secure and compliant. Any interruption, unintended disclosure or data loss from databases has the potential to disrupt an entire company's operations and damage its reputation.

Compliance officers and regulators understand the importance of database security and are watching it closely these days. And what they're seeing continues to raise concerns: companies have invested in firewalls, data loss prevention (DLP) tools, and native database auditing tools, yet they continue to fail compliance audits. Here are some of the most common compliance audit flags involving databases:

- *Database misconfiguration issues*—Change is good, right? Not when it comes to database system configurations. Database administrators need the ability to audit and validate configurations, ensuring reliable operation by enforcing a gold standard configuration and preventing unauthorized changes from taking place.
- *Security patches are available, but not applied*—With dozens of critical updates and vulnerabilities being disclosed each week, it's understandable that many companies delay patch deployment. However, one of the first tests conducted during a security audit is to determine whether databases have all patches currently applied.
- *Security patches are unavailable*—Many companies continue to run databases that have reached end-of-life status, such as Oracle 8i, Oracle 9i, Oracle 10g, and Microsoft SQL Server 2000. Vendor patches are no longer available for these systems.
- *Inadequate enforcement of user account management and segregation of duties policies*—It's not enough to have user access controls and segregation-of-duties policies in place—they must be continuously and automatically enforced

Databases are 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.

Challenges

Old habits don't address new realities—or compliance requirements

It's a common pattern for companies to secure the enterprise at the network level and hope for the best. However, compliance auditors and regulators don't share this viewpoint. They know the limitations of perimeter security, know the risks of insider threats, and have seen first-hand the damage caused by lax database security.

Perimeter-based defenses may provide a superficial (and ultimately false) sense of security, but they are hardly a fail-safe method of securing the enterprise. Database security point solutions may help, but they have inherent limitations. For starters, most are vendor-specific or function-specific. That is, they may be just for Oracle or Microsoft or IBM databases, and they only cover limited, disjointed portions of the database security puzzle. Even after fully implementing database point products, organizations struggle with aggregating and correlating data from them. In many cases where databases from multiple vendors are scattered throughout the enterprise, organizations don't even know they are running a particular database, and coverage is spotty at best.

The bottom line is databases require more protection than they're receiving today:

- Companies often store their most critical, sensitive data in databases
- Ninety-six percent of security breaches involving company records occur through databases[1]
- More than half of database breaches originate from within companies

Database managers are obsessive about availability and performance

Because databases are constantly in use and critically important, database administrators like to create "gold standard" database configurations that are built for performance and availability. They are very reluctant to alter these configurations, patch databases, or add "performance-killing" security software to their servers.

Management can't bear to write off outdated investments

You can't blame them. When a company has invested heavily in point products, the tendency is to hope for the best and expect that by adding just one more stop-gap solution, everything will be fine. The problem with that approach is that it's hard to see the big picture—a picture that just might reveal gaping holes between costly one-off solutions. And yet the reality is, you can't afford to be hacked. Investing in a comprehensive security solution that protects your data, database access, network, and associated servers and endpoints is likely to cost a fraction of a serious breach.

Every patch announcement increases your vulnerability

The most critical period of vulnerability extends from the time that database management system (DBMS) vendors issue a security patch until it is applied. During this window of golden opportunity, hackers know about a weakness and that it is likely to be exploitable for quite some time.

However, applying patches is easier said than done. Companies often have hundreds of databases and limited patch deployment resources. Even when resources are available, databases must be brought down for patches to be installed, and the database must undergo regression testing before it can be brought back online.

Hackers rise to the occasion and work to exploit whatever vulnerabilities they can. What's more, with the automation tools used by hackers and the widespread sharing of information over social networks, the frequency and sophistication of database attacks is going through the roof. Patch Tuesday continues to be a very opportunistic time for hackers and crunch time for database administrators (DBAs).

Firefighting works for firemen, not auditors

Most organizations know they need to comply with applicable regulations, such as PCI-DSS, SOX, HIPAA/HITECH, EU Data and Privacy Directives, local and state privacy protection laws, and/or any other information security mandates that may affect their industries. Database vendors' native controls are largely inadequate, and their additional security overlay point products, designed only for their database management systems (DBMS), often have very negative impacts on system performance and availability. Moreover, they do nothing to address the pressing need to centrally manage extensive, heterogeneous database environments.

Advanced persistent threats and cybercrime

Today, online identity data is more vulnerable than ever before. Crackers and cybercriminals have adopted methods that are stealthy and targeted, commonly referred to as advanced persistent threats, or APTs. These attacks slowly and methodically exploit network, operating system, and, finally, database layers before they succeed in stealing your data. APTs are not flashy like denial-of-service attacks or web page defacement. Unfortunately, one product cannot secure against these kinds of attacks.

Cybercrime is another major concern if your organization possesses valuable intellectual property or is hosting confidential information that may be beneficial to competitors or even foreign governments. Corporate espionage has become very lucrative and increasingly prevalent. In 2012, FBI Director Robert S. Mueller III warned, "Cyberattacks would soon replace terrorism as the agency's number one

concern, as foreign hackers, particularly from China, penetrate American firms' computers and steal huge amounts of valuable data and intellectual property."[2]

Many of these attackers have lots of resources at their disposal. To counter this, organizations need comprehensive strategies in place to combat multiple threat vectors and secure the entire security stack from network to operating system to database. However, the most important action item involves implementing a solution that provides a holistic view of your security posture and not just database security.

Controlling privileged users

Whether by malicious or accidental activities, insider threats are drawing increased attention by auditors and regulators. In the 2012 *Aftermath of a Data Breach* study, conducted by the Ponemon Institute, investigators found that insiders and third parties are the most common cause of data breaches. Of the incidents that were successfully traced to a root cause:

- Thirty-four percent were attributed to negligent insiders
- Nineteen percent were traced to third-party data outsourcers
- Sixteen percent were traced to malicious insiders

Solutions

Securing the database environment: a more holistic approach to security and compliance

Native database security features are too fragmented and labor-intensive to effectively defend large, heterogeneous environments, and they inevitably impose a substantial penalty on system performance. Perimeter defenses alone can't stop sophisticated attacks against database-specific vulnerabilities or prevent improper access by privileged insiders. So, what does a comprehensive but practical database security solution look like? What are the essential features, functions, and characteristics?

At McAfee, we believe that successful and sustainable database security and compliance require a layered approach that provides:

- Global visibility into the organization's database assets and vulnerabilities across all vendors and technology platforms
- Activity monitoring and policy enforcement that do not impose an additional workload on the databases themselves
- Reliable controls and audit records that ensure proper segregation of duties so that even privileged users cannot bypass security
- Scalability and extensibility to virtualized and cloud environments.

Let's take a level-by-level look at what's required to render an enterprise database environment secure and compliant—and the McAfee technologies that make database security a practical reality.

Discover Databases and Operating Systems on Your Network and Assess Vulnerabilities

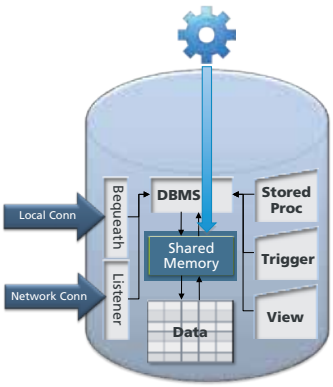
McAfee® Vulnerability Manager for Databases

To secure a database environment, you have to be aware of all of your database assets and their current configuration states. You must be able to automatically discover all the databases on your network regardless of vendor or technology platform, collect a full inventory of their configuration details, determine if the latest patches have been applied, and test for common weaknesses. These capabilities are fundamental to any effort to demonstrate regulatory compliance and ensure data security, and in the McAfee solution stack, they are delivered by McAfee Vulnerability Manager for Databases.

McAfee Vulnerability Manager for Databases automatically discovers databases on your network and conducts more than 4,700 vulnerability checks across leading database systems, including Oracle, Microsoft SQL Server, IBM DB2, MySQL, and others. It evaluates risks from virtually every threat vector, determines if the latest patches have been applied, and tests for common weaknesses, such as weak

Memory-Based Sensors Make a Difference

McAfee Database Activity Monitoring uses intelligent, autonomous agents to monitor all database activity in memory (shared or cache). This unique approach provides full visibility into all database activity, including intra-database activity and obfuscated payloads. Because the sensor can identify such transactions in memory, and since it resides on the host, it can block them instantly.



passwords and default accounts, as well as the presence of sensitive data such as credit card or Social Security numbers that are in clear text. In addition, it sorts and prioritizes scan results and provides fix scripts and remedial recommendations.

McAfee Vulnerability Manager for Databases is developed and maintained by the same team credited with contributions to seven of the last 10 critical patch updates released by Oracle. It leverages the expertise of leading database practitioners to:

- Identify susceptibility to database-specific risks, including SQL injection, buffer overflow, and malicious or insecure PL/SQL code
- Prioritize findings and highlight the "real" issues that require immediate attention
- Provide actionable intelligence on how to address risks, including fix scripts whenever possible
- Allow security and compliance users with limited database knowledge to quickly understand risks to sensitive data and how to remediate them

By providing global visibility into database vulnerabilities, McAfee Vulnerability Manager for Databases sets the stage for effective database security and efficient, affordable compliance.

McAfee Vulnerability Manager for Databases can quickly discover and reconcile assets running on your network. Not only does it identify the running services, operating systems, and network devices, it also provides a platform to implement and manage vulnerability lifecycle management. If a database is secure but the operating system on which it is running is not secure, then your database is at risk. To reduce the risk, it is critically important to assess and manage it at the operating system and network layer. McAfee Vulnerability Manager for Databases comprehensively assesses multiple operating systems, network devices, and workflows for vulnerabilities and mitigate those vulnerabilities.

McAfee Change Control provides essential network configuration assessment capabilities. It assesses the network configuration and stores it. What's more, you can quickly roll back the network configuration if it is not the optimal configuration.

Monitor Activity for Changes and Manage the Extended Database Environment

McAfee Database Activity Monitoring

True security can only be achieved when operations are efficient and database protection is a smooth, consistent part of the process. IT managers must have the right tools in place to identify and protect assets and can view what is happening in every corner of the enterprise in near real time from a single software platform that enables management and monitoring across endpoints, networks, and databases.

To be effective, the solution must monitor all database behavior and activity from a vantage point outside of the database. Otherwise, database administrators could disable the function (deliberately or inadvertently). A solution must be able to terminate a session that violates a policy, generate alerts to a centrally managed console, and quarantine a malicious or non-compliant user.

McAfee Database Activity Monitoring accomplishes all of this and more. It automatically finds databases on your network, protects them with a set of preconfigured defenses, and helps you build a custom security policy for your environment—making it easier to demonstrate compliance to auditors and improving protection of critical data assets.

McAfee Database Activity Monitoring uses a unique, software-based approach to monitoring database activity. Non-intrusive, memory-based sensors observe activity locally on each database server and identify malicious behavior whether the attack vector is across the network, a local privileged user, or a procedure stored within the database itself.

This approach doesn't require any database or host downtime, generate any latency, or consume any database I/O. Real-time monitoring and intrusion prevention capabilities stop breaches before they can cause damage. When a policy violation occurs, an alert is sent directly to the monitoring dashboard with full details to guide remediation. High-risk violations can automatically terminate suspicious sessions and quarantine malicious users.

McAfee Virtual Patching for Databases

McAfee Virtual Patching for Databases shields databases from the risk presented by unpatched vulnerabilities by detecting and preventing attempted attacks and intrusions in real time, without requiring database downtime or application testing. Virtual patching delivers protection against known vulnerabilities and SQL injection attacks on unpatched databases. All database commands are monitored in memory, based on predefined rules. Once these rules are triggered, the attacks can be blocked by terminating the session, user, or IP address. In addition to providing a reliable audit trail, it also delivers virtual patching updates on a regular basis for newly discovered vulnerabilities. And it lets you implement virtual patching without database downtime—protecting sensitive data until a patch is released by the database vendor and you are ready to apply it.

According to the Aberdeen Group, "Companies should give strong consideration to virtual patching as a strategy to augment their traditional patch management process, and to improve the overall efficiency and effectiveness of managing vulnerabilities and threats to their IT infrastructure."[3]

"The strategic deployment of selective compensating controls, such as virtual patching, can provide a kind of protective shield that effectively buys an organization more time to assess, plan, test, and remediate vulnerabilities and threats."

The Virtues of Virtual Patching, Aberdeen Group, October, 2012

McAfee® ePolicy Orchestrator® software: end-to-end security visibility and control

The McAfee Database Security Solution is integrated with McAfee ePolicy Orchestrator (McAfee ePO™) software, the industry's number one security management platform. McAfee ePO software is widely acknowledged as the most advanced and scalable security management platform available today. With McAfee ePO software, organizations of all sizes can efficiently manage any number of devices—all from a personalized web console that provides a single, interactive "pane of glass" viewpoint for administration, policy, analysis, reporting, and alerting. As a key component of the McAfee Security Management Platform, McAfee ePO software manages security across endpoints, networks, and data; integrates third-party solutions; and automates workflows and role-based reporting to create efficiencies, streamline compliance, and provide visibility into security and compliance postures.

Security Connected

The Security Connected framework from McAfee enables integration of multiple products, services, and partnerships for centralized, efficient, and effective risk mitigation. Built on more than two decades of proven security practices, the Security Connected approach helps organizations of all sizes and segments—across all geographies—improve security postures, optimize security for greater cost effectiveness, and align security strategically with business initiatives. The Security Connected Reference Architecture provides a concrete path from ideas to implementation. Use it to adapt the Security Connected concepts to your unique risks, infrastructure, and business objectives.

The Business Case for Virtual Patching

Virtual patching is a proven approach to protecting databases and operating systems that is approved as valid compensating control by compliance regulators. Applying a virtual patching solution allows businesses to:

- Deploy patches on their own regular patching cycle
- Eliminate the need to bring operational databases offline for updates each time a patch is released
- Reduce the need for emergency patch workarounds
- Provide a valid security and compliance solution if they are running legacy databases

McAfee: The Right Database Security Partner Right Now

Mission-critical databases are the lifeblood of most organizations. Their stability and performance have always been high priorities for IT departments. Security has been important, too. However, now those same databases are high-priority targets for nefarious activities. This evolving threat reality means that conventional defenses are inadequate when measured against the intellectual power of today's cybercriminals.

To better secure your essential business data, McAfee delivers a complete database security solution that protects your entire database environment efficiently and cost effectively, while maintaining optimum system performance and availability. This comprehensive solution secures all leading databases and every server and byte of data that touches them. The McAfee Database Security Solution Architecture is highly scalable and extensible to virtualized and cloud environments. The integrated components bring to bear the industry's most complete and fully integrated portfolio of information security technologies and services with the global threat intelligence of McAfee Labs to best protect your sensitive data assets. And they are vital components of the Security Connected framework from McAfee, which helps you optimize security each day, enabling your business while reducing risk, driving compliance, and realizing operational efficiencies.

For more information, visit www.mcafee.com/dbsecurity, or contact your local McAfee representative or reseller near you to see if you qualify for a free evaluation of the McAfee Database Security Solution.

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), is the world's largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by its unrivaled global threat intelligence, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. McAfee is relentlessly focused on constantly finding new ways to keep our customers safe. http://www.mcafee.com.

[1] *2012 Verizon Data Breach Investigations Report*
[2] U.S. House Appropriations Subcommittee testimony, March 7, 2012
[3] Aberdeen Group Analyst Insight: *The Virtues of Virtual Patching*, October 2012

McAfee
An Intel Company

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

60090wp_database-security_0313_fnl_ETMG