PROTECT YOUR DATABASES

Boost security against today’s attacks and loss vectors
Boost security against today’s attacks and loss vectors

The Situation
According to the 2013 Verizon Data Breach Investigations Report, the 47,000+ security incidents in 2013 represented the largest ever covered in any single year, including 621 confirmed data disclosures and at least 44 million compromised records. And unfortunately, most of these incidents go unnoticed by the involved organization. The report goes on to say: “approximately 70% of breaches were discovered by external parties who then notified the victim.”

So the records keep getting compromised, data continues to be exposed, and most often the organization has no idea the incidents even happen until someone else tells them.

Unfortunately, attackers sometimes get unintentional help from employees. Through social engineering and credential theft, attackers can find ways to look like “insiders” with legitimate access. In addition to the unknowing or unintentional exposure that leads to privileged access, since database assets are so commercially and strategically valuable, bribery can work, too. So you can’t trust your perimeter protections to keep your database safe, and you can’t completely trust that all your employees will always do the right thing.

Driving Concerns
Databases not only store critical information, but they are often connected to multiple systems providing essential business services. Any interruption, unintended disclosure, or loss of data from databases has the potential to disrupt an entire company’s operations and reputation. Also, since a database holds the regulated and sensitive data, a database breach usually translates to a compliance breach, with its associated cleanup costs, loss of consumer confidence, and possibly drastic market capitalization loss.

To secure sensitive data against both external and internal threats, real-time visibility into database activity is required. Most organizations today leverage logging and auditing tools inherent in the database to provide this protection, but these tools are woefully inadequate against modern hacking and social engineering tactics. In order to properly secure a database from malicious code and data loss, you must address these concerns:

• Discovery of all databases within the enterprise. You can’t protect something if you don’t know it exists. Building solid security around databases begins with two important steps: finding them all, and then figuring out where the associated weak spots are. Almost all organizations are challenged with locating and identifying all their databases across the enterprise. And even when they are able to locate and identify some of them, conventional vulnerability assessment products aren’t comprehensive and intelligent enough to thoroughly test database systems, potentially putting your most sensitive and valuable data at risk.

• Monitoring activity for unauthorized access. All databases respond to commands. As long as a command is appropriate for the user requesting data, it will be successful. As attacks and tools become more sophisticated, attackers can evade typical detection techniques and escalate privileges. Weak access controls make the job of an attacker even easier. Typically, the level of access granted to users
far surpasses the access rights that they need on the system or require for their roles. Stale accounts and lax control over new account creation allow more doors for attackers to knock on. They first attack default and weak passwords and then escalate privileges. Network-based activity monitoring has proven to be inadequate against this issue, since local access methods can bypass network-based monitoring systems.

• **Auditing tools.** The native logging and auditing capabilities of databases fall far short of providing the right visibility. Most will not capture changes made, privileges used, respective administrators, or any system-level changes. Further, logging and auditing activities integrated within the database can hinder database performance. Designed for monitoring, not security, administrators can also turn these features off, eliminating any value the native tools might have provided.

• **Avoid downtime from patching.** Operational availability, particularly with respect to mission critical databases, is crucial. Some organizations have a patch cycle of well over 12 months. There are hundreds of new threats each year, but due to the critical nature of databases, downtime is often not an option. In addition, many databases are no longer actively supported by the respective vendor, so patches are no longer available. Organizations need to be protected continuously without requiring patching of the database.

• **Cloud ready.** As organizations shift more mission-critical services to the cloud, each database must adapt to be accessed and monitored using cloud services, not just over the local network.

• **Proof of compliance with industry, government, and internal standards.** Depending on the role of your database, it may need to adhere to, report against, and maintain policies for a range of U.S. regulations, such as PCI DSS, Sarbanes-Oxley, HIPAA, GLBA, and FISMA. Other countries have their own privacy and financial control requirements as well. In addition, your organization may have developed its own best practices and operating standards, and executives expect dashboards showing status against governance standards.

**Solution Description**

Every organization relies on a database for its operations. If we don’t rely on operating system vendors to protect their operating systems, why do we settle for vendor-supplied tools to help us secure our most valuable database assets? Databases have unique challenges and typically have been left in the hands of database administrators to implement security policies and standards. With the number of database breaches in the headlines, a new approach must be considered that can ensure the integrity of databases is protected against malicious code and—sad but true—our own trusted insiders.

To address these concerns, a solution must be able to meet these requirements:

• **Database discovery.** Tools can help you scour the network to locate any and all databases, identify the ones that contain sensitive data (such as 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. 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 drift from the approved baseline.

• **Monitoring activity and unauthorized access.** A solution must be able to monitor all database behavior and activity from a vantage point outside of the database. If this monitoring were performed solely within the database, database administrators could disable the function (deliberately or inadvertently). A solution must also be able to terminate a session that violates a set policy, generate alerts to a centrally managed console, and quarantine a malicious or unauthorized user. A solution must be able to detect evasion techniques and prevent them from compromising the system.

• **Auditing tools.** Similarly, auditing tools are ineffective if an administrator can disable them. A solution must be able to provide protected audit and logging capabilities to ensure records are captured and available for analysis. During post-incident forensic analysis, this audit trail can help you understand if there was an incident, verify if any data was compromised, and gain greater insight into malicious activity. A solution must be able to provide an audit trail and reports that can meet SOX, PCI, HIPAA, FISMA, and other compliance audit requirements.
• **Patch when it's suitable.** Waiting for the database vendor to supply a patch or skipping patches to avoid productivity loss leaves your databases vulnerable to many threat vectors. A virtual patch concept can help protect against zero day and newly discovered vulnerabilities and can be implemented without database downtime, protecting sensitive data until a patch is ready to be applied. In addition, virtual patching is often considered a compensating control with respect to regulatory compliance.

• **Cloud ready.** Relying on analysis of network traffic to identify policy violations is either impossible or inefficient in the highly dynamic and distributed architectures used for data center virtualization and cloud computing. A solution should be able to automatically provision sensor configuration for each new database instance, request the affiliated security policy based on the data it hosts, and then begin sending relevant rule-based alerts to the management server. Even if network connectivity is interrupted, data should still be protected via locally enforced policies.

• **Complying with industry, government, and internal standards.** As standards and regulations change, so do the reports that you must maintain. A solution must provide compliance and regulatory templates that are maintained with the latest controls and violation guidance. A solution must be able to identify threats as they occur, and report on prevention, reducing risk and liability. Pre-configured templates should include PCI-DSS, Sarbanes-Oxley, HIPAA, and GLBA, all viewable from within a centrally managed platform.

**Technologies Used in the McAfee Solution**

McAfee offers the following products specifically designed for database security: McAfee® Vulnerability Manager for Databases, McAfee® Virtual Patching for Databases, and McAfee® Database Activity Monitoring. Complete integration with centralized management through McAfee ePolicy Orchestrator® (McAfee ePO™) ties this suite of products into a unified database security and compliance management platform for your entire infrastructure.

McAfee Vulnerability Manager for Databases conducts more than 4,700 vulnerability checks against leading database systems, including Oracle, Microsoft SQL Server, IBM DB2, Sybase, and MySQL. By improving visibility into database vulnerabilities and providing expert recommendations for remediation, McAfee Vulnerability Manager for Databases reduces the likelihood of a damaging breach, and saves money through better preparation for audits and compliance with regulatory mandates. McAfee Vulnerability Manager for Databases helps to reduce the attack surface by identifying typical weaknesses that hackers and attacks look for, such as weak passwords, shared passwords, and default accounts. To help you track and respond to suspicious events, it will report back version/patch level, changed objects, modified privileges, and forensic traces from common hacker tools.

Virtual patching is a way to protect the database against exploits without modifying any of the database server binaries. McAfee Virtual Patching for Databases periodically and automatically updates the databases' security posture as soon as new threats are identified without incurring costly business disruption and database downtime required by traditional patching methods. It is also an effective means for protecting databases that are no longer supported by the vendor.

Unlike historical auditing or log analysis, which can only tell you what happened after the fact, McAfee Database Activity Monitoring provides real-time visibility and intrusion prevention capabilities to help stop breaches before they cause damage. More than 380 predefined rules address specific issues patched by the database vendors, as well as generic attack profiles. Pre-built policy templates can be customized to support rules for appropriate and compliant database access and processes.
Alerts are sent directly to the monitoring dashboard with full details of any policy violation for remediation purposes. Policies for violations deemed to be high risk can be configured to automatically terminate suspicious sessions and quarantine unauthorized users, allowing time for the security team to investigate the incident.

Attacks targeting valuable data stored in databases can come from across the network, from local users logged into the database server, and even via stored procedures or triggers from inside the database itself. McAfee Database Activity Monitoring uses memory-based sensors to monitor activity and catch all three types of threats with a single, nonintrusive solution. Virtual patching updates are provided on a regular basis for newly discovered vulnerabilities and can be implemented without database downtime, protecting sensitive data until a patch is released by the database vendor and can be applied. Activity and event information can then be used to demonstrate compliance for audit purposes and to improve security overall.

Specialized protections allow McAfee to assess database vulnerabilities and monitor for malicious and risky actions.
McAfee Vulnerability Manager for Databases
Designed to speed initial scans and out-of-the-box reports to address most compliance requirements, McAfee® Vulnerability Manager can discover and scan multiple databases from a single console. It will locate and identify tables containing sensitive information and conduct a quick port scan providing database version and patch status. In addition to basic password strength detection (simple, default, and shared passwords), it can scan hashed passwords, and will also test for susceptibility to database-specific risks, including SQL injection, buffer overflow, and malicious or insecure PL/SQL code. It then presents the findings in preconfigured reports in compliance with various standards, frameworks, and regulations.

McAfee Virtual Patching for Databases
McAfee Virtual Patching for Databases non-intrusively protects unpatched database servers from known vulnerabilities, and all database servers from zero-day attacks based on common threat vectors, without application testing or having to take the database offline to patch it. In addition, it is the only solution for those older database versions that are no longer supported by the respective vendors, and has been approved by auditors as an acceptable compensating control.

McAfee Database Activity Monitoring
McAfee Database Activity Monitoring is a small footprint sensor, a software agent that is installed on the database host server itself and monitors all activity. The sensor is a standalone process written in C++ and running on the database host machine. It is installed using standard platform tools (RPM, PKG, DEPOT, BFF, or EXE) in a separate operating system user account on the system. The sensor automatically identifies all database instances on the machine and can monitor multiple virtual instances, even different database types, on the same host.

When running, the sensor attaches itself to the instance memory area of the SQL cache, using read-only mechanisms and application programming interfaces (APIs), and begins monitoring by a polling loop of memory sampling. For every sample cycle, the sensor analyzes currently running and previous statements for each session in the database instance and, using a predefined policy received from the server, determines what statements should be alerted on or blocked. Statements violating the policy are sent to the management console in real time as alerts. The sensor can also be configured to terminate sessions on specific violations and to quarantine users. It is non-intrusive and consumes only small amounts of CPU resources (less than 5 percent of a single CPU core, even on multi-CPU machines). The sensor prevention capabilities are implemented using native database APIs that allow it to terminate database sessions without introducing any risk to data integrity. It can be directly managed from the McAfee ePO platform, providing configuration, policy management, and centralized reporting and summary information for thousands of databases within a single, consistent dashboard.
McAfee ePolicy Orchestrator (McAfee ePO)
McAfee ePO enables centralized, automatic software distribution, configuration, and policy management of the McAfee Database Security solution. McAfee Vulnerability Manager for Databases, McAfee Virtual Patching for Databases, and McAfee Database Activity Monitoring are all fully integrated and centrally managed from the McAfee ePO console, providing centralized reporting and summary information for all your databases. This complete integration with McAfee ePO delivers a common deployment and policy control point, single “pane of glass” view, and streamlined reporting. For example, database instances appear as part of the ePO system tree, allowing the assignment and management of multiple discrete policies and rule object definitions for individual databases and system tree groupings. In addition, associated rules can be dynamically applied for specific alerts and threat mitigation techniques, while delivering consolidated and individual database assessment scanning and activity dashboard views and reports.

Impact of the Solution
By introducing unique protections for the attacks and data loss vectors specific to databases, you can improve your ability to detect and fend off external attacks, and also reduce the chance of compromise or disruption originating from within the organization’s infrastructure.

McAfee provides real-time visibility and protection from all sources of attacks by monitoring and alerting on suspicious events. Whether the threat comes from across the network, from local users logged into the server itself, or from inside the database, McAfee helps to minimize risk and liability by stopping attacks before they cause damage. Virtual patching of newly discovered database vulnerabilities, or from vulnerabilities in databases that are no longer supported by the vendor, provides immediate and automated protection with no database downtime.

Pre-defined templates and rules, automated and updated checks, and wizard-based interfaces speed deployment and help you achieve an efficient and easily auditable database security architecture.
Additional Resources
www.mcafee.com/dbsecurity
www.mcafee.com/vmfordatabases
www.mcafee.com/dbactivitymonitoring
www.mcafee.com/virtualpatching
www.mcafee.com/epo
www.mcafee.com/vm

For more information about the Security Connected Reference Architecture, visit:
www.mcafee.com/securityconnected