White Paper

A Practical Guide to Database Compliance

Preserve your organization's integrity by securing sensitive information

Table of Contents

Why is database security so important? For a company that has suffered a serious data breach, it boils down to monetary and reputation damage in many forms—business disruption, bad publicity, stiff fines for noncompliance, and undermined confidence with the existing base of customers, partners, and employees. But most damaging of all is the trouble that it creates when it comes to signing up new customers. When a company's reputation has taken a beating, a data breach creates a steep hill for sales and business development to climb. That's why data security in general and database security in particular are a crucial part of any company's overall corporate health.

The Pain and the Price

Think database and data security aren't really that important? Just ask the folks at Yahoo! and LinkedIn. In 2012, both of these companies were victims of widely publicized data breaches. Yahoo! saw roughly 450,000 sensitive records compromised. Approximately 6.5 million passwords were leaked out of LinkedIn.

In early 2009, Heartland Payment Systems, which processes payroll and credit card payments more than 250,000 businesses, reported that consumer credit card data was exposed in a security breach of historic proportions.

What cut even deeper was the admission by Heartland at the time that it couldn't pin down exactly when the malware responsible for the breach had penetrated its system. It was apparent, however, that the breach had most likely taken place sometime in late October or early November, some two and one-half months before Heartland's disclosure. According to published reports, Visa and MasterCard—two of the major credit card companies that use Heartland for processing—had reported anomalies to Heartland in late October.

Visa, however, took further public action against Heartland by removing the company from its list of Payment Card Industry Data Security Standard (PCI DSS) compliant service providers. Visa also placed Heartland on probation with the Visa transaction processing network. Heartland was able to continue to process card transactions but had to submit to more stringent security assessments, monitoring, and reporting.

Clearly, the potential harm to consumers, merchants, and banks—and the possibility of multiple class action lawsuits resulting from the breach—created the profile of a painful, time-consuming, and costly experience.

The combination of damaging and highly publicized data breaches and stricter regulatory compliance demands continue to push database security to the foreground. Even at this late date, database security still has an aura of mystery about it, almost as though it were a "black art." Part of the mystery is driven by two simple facts: many database professionals are not familiar with the security aspects of database management, while a large number of security professionals have a grasp of desktop security but not database security. This is beginning to change as the importance of securing databases becomes more and more apparent.

Understanding the Threat

Databases are subject to some unique types of threats that cannot be handled by firewalls, intrusion detection and prevention systems, and other perimeter defenses. Even the basic set of security features typically offered by database vendors (primarily access control in the form of username/password login credentials) can be easily bypassed by a knowledgeable insider with malicious intent, or by a sophisticated hacker. The threat landscape is constantly evolving and becoming more sophisticated and specialized (for example, attacking through backdoors inserted inside databases). Furthermore, database administrators typically do not devote anywhere near enough attention to security matters, so in the absence of proper personnel to manage this function, obvious vulnerabilities will be overlooked and ultimately exploited.

Who are the intruders?

The profile of the typical hacker has changed dramatically over the last few years. The stereotyped image of the brilliant young loner who hacks into a secure environment for the sake of mischief and mayhem has given way to a different and more insidious threat: members of organized crime syndicates who seek profit and prefer long-term stealth to short-term drama. In the end, this new type of cyberfraud professional is much more damaging. The changing profile and purpose of the intruder has reshaped the nature of intrusion attempts from ones that try to penetrate, and then perhaps deface or wreak havoc, to ones that strive to be stealthy and leave no tracks with the aim of stealing data for financial gain.

Insider threat, privileged users

Concurrently with the change in the nature of the external threat, there is increasing attention being given to the "insider threat." This umbrella term refers to damage caused by individuals within the organization, either maliciously or accidentally.

Is the insider threat serious? It certainly is. You need look no further than the Ponemon Institute's 2012 *Aftermath of a Breach Study* for proof. The organizations surveyed determined that 16 percent of the breaches suffered were at the hands of malicious insiders. Furthermore, It was found that an additional 34 percent of breaches were due to insiders. In some cases, insiders freely revealed their administrative passwords, creating easy access to sensitive data for attackers bent on doing financial harm. And while stolen credentials were the most common way for attackers to gain access to data, the theft was often committed with the help of an "inside assist."

While it should be clear that not all insiders are suspects, it is just as apparent that insiders bent on stealing data have a greater chance of succeeding than those engaged in outside intrusion attempts.

The criminalization of the general threat landscape also has an impact on "crimes of opportunity" committed by insiders. It is often easier and quicker to offer a bribe to an insider who already enjoys access privileges than to attempt hacking from the outside. In response to the significant risk posed by insider involvement in database breaches, the Defense Advanced Research Projects Agency (DARPA) launched a project for detecting and responding to insider threats on US Department of Defense Networks.

Still feeling the sting of the WikiLeaks disclosures, which caused such embarrassment for the US Department of Defense, DARPA will use the Cyber INsiDER (CINDER) threat program to look for ways to improve the speed and accuracy of insider threat detection. DARPA will focus on looking for telltale signs and network activities that should be monitored to detect malicious activity.

Many regulatory compliance requirements focus on privileged insiders as well, with special attention given to those whose actions used to go unmonitored in the past.

Vulnerabilities

As database management systems have grown in complexity, they have become more vulnerable to attacks. The nature of these vulnerabilities ranges from the relatively benign to weaknesses that allow unauthorized users to bypass the built-in access control mechanism of the database, escalate access privileges, and hijack the database. Privilege escalation attacks are relatively common, and can occur when a user—either from outside or inside the organization—is able to achieve additional access to the database system beyond his/her level of authorization. This feat is achieved by exploiting vulnerabilities within the database management system. Once elevated access is gained by a rogue user, they can access sensitive data within the database, run procedures or native programs, and can even fully take over the system to wreak havoc.

Much has been said and written about how DBMS vendors should cope with vulnerabilities and how quickly they should develop patches for them. The reality over the past few years is that the number of reported vulnerabilities is constantly rising, despite the fact that vendors are doubling their efforts to patch them.

Additionally, it usually takes a vendor several months or more to distribute a patch, and it takes an additional several months for customers to install the patches. The patch installation process usually requires testing and database downtime. For these and other reasons, many customers do not apply the patches at all, and their databases remain vulnerable to severe attacks.

Existing Solutions Are Inadequate

Perimeter security

When it comes to databases, the traditional perimeter defenses such as firewalls and intrusion detection systems/intrusion prevention systems (IDS/IPS) are grossly inadequate due to the sophisticated nature of the threats posed to databases and the specific nature of their vulnerabilities.

While many intrusion prevention systems claim to thwart SQL injection attacks, for example, their capabilities in this area are very weak and are usually based on signatures, which hackers can easily evade. IPSs are certainly incapable of detecting sophisticated attacks that exploit vulnerabilities that are specific to database software from a particular vendor and to a particular version of the DB and platforms that are supported by the DB software.

Native DBMS auditing

Virtually all database management systems have the ability to write audit logs for some or all transactions. However, they are seldom used extensively due to the detrimental effect they have on database performance and the amount of storage they need for full auditing. From a security standpoint, the usage of open logs is inadequate anyway since the logs can easily be manipulated after the fact and privileged users can turn the audit function on and off as they please.

Compliance and Security

Compliance requirements for databases

There are many different compliance laws and regulations nowadays. The compliance landscape has evolved over the recent past and changed the way many IT systems, applications, and data are controlled. Here are brief descriptions of the key regulations and their effect on database management and security practices.

Sarbanes-Oxley

The Sarbanes-Oxley legislation of 2002 (SOX) forced publicly traded companies to be more transparent about their financial data. This is a federal law and does not specify technical measures or tools that enterprises should use, but rather requires them to have "effective controls" in place. Specifically:

- Section 302 of SOX requires executives to certify the accuracy of financial reports. This means that company officers must have a handle on how data is flowing to create the reports. They must be certain that the data cannot be seen by unauthorized personnel, altered without authorization, or otherwise tampered with.
- Section 404 of SOX further requires executives and auditors to confirm the "effectiveness of internal controls." While the exact nature of internal controls is not specified, auditors commonly put particular emphasis on:
  - » Ensuring the integrity of sensitive data
  - » Activity of privileged insiders
  - » Traceability of data (audit trail)
  - » Separation of duties (audit independence)

Obviously most of the financial data resides in databases in one form or another, so SOX auditors are increasingly looking for ways to view database activity in a way that can be easily interpreted and acted on.

SOX does assess serious criminal penalties for noncompliance when it comes to financial reports. SOX auditors require companies to establish, enforce, and validate "segregation of duties" with respect to access/changes to financial data stored in a company's database (for example, access only by authorized personnel). In particular, corporate officers who knowingly certify a statement that doesn't adhere to SOX compliance standards can be fined a maximum $1,000,000 or face a maximum prison sentence of 10 years, or both. If they do the same thing willfully, they can face a maximum $5 million fine or 20-year prison sentence or both.

PCI DSS 2.0

The Payment Card Industry's Data Security Standard (PCI DSS) is the result of the joint efforts of the major credit card companies. It is not legislation nor regulation, but rather a standard, and it periodically gets updated (so far, once a year). The standard compels merchants and companies that process and store credit card data to comply with a set of technical and procedural requirements, and pass audits. Unlike SOX, PCI gets specific about what measures need to be put in place for protecting credit card data. Inability to comply carries stiff penalties from the credit card companies, and, if not rectified, eventual withdrawal of the right to conduct business with the credit card companies. While PCI DSS is not really a regulation or legislative act, it does carry some monetary pain for noncompliance. Penalties for noncompliance include fines ranging from $5,000 to $100,000 per month (at the discretion of the particular payment brand), as well as increased auditing requirements.

Of particular interest is the concept of "compensating controls" (section 3.4), which recognizes that cardholder data encryption is sometimes not possible or would take a long time to implement. It allows for a combination of other methods to be used instead, including real-time monitoring of database access to identify and prevent unauthorized access to credit card data.

CA SB1386 and similar privacy breach notification laws

The majority of states in the US, plus the District of Columbia, Puerto Rico, and the Virgin Islands have enacted privacy breach notification laws similar to California Senate Bill 1386. Some observers have been pushing for a federal law, but others have argued that the individual state laws are doing a good job of handling the issue. While the US House of Representatives has passed HR 2221, the Data Breach Accountability and Trust Act, the US Senate has not taken action on the House bill, so a Federal data breach law still does not exist. These laws compel organizations to notify the authorities and affected individuals whenever a breach of personal identifiable information (PII) is exposed, such as Social Security numbers.

HIPAA/HITECH

The Health Information Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) Act are Federal laws that were put in place to ensure that the freedom of patients to choose healthcare insurers and providers will not come at the expense of the privacy of patient medical records.

The HIPAA articles relevant to securing database are mainly the following:

- § 164.312(a)(1): Access Control, which requires organizations to "Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights"
- § 164.312(b): Audit Controls, which requires organizations to "Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information"
- § 164.312(c)(2): Integrity, which requires organizations to "Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner"

Although HIPAA had been notorious for weak enforcement, recent legislative action has altered the picture. When the American Recovery and Reinvestment Act (ARRA) of 2009 was signed into law, it included a strong healthcare component. The Health Information Technology for Economic and Clinical Health Act (HITECH Act), a key part of ARRA, has also become law and will turn up the heat on both penalties and enforcement for HIPAA compliance.

A key element of the new framework is that enforcement authority for HIPAA security rules has been transferred from the Centers for Medicare and Medicaid to the Office of Civil Rights, which has more resources to bring to the fight. According to published reports, the Office of Civil Rights—which has 275 investigators and a $40 million budget—is in a much better position to crack the enforcement whip.

SSAE 16

The Statement on Standards for Attestation Engagements (SSAE) No. 16 is an auditing standard for the service industry that allows auditors to certify that a service company has the appropriate controls in place to safeguard customer data. It was put into effect in June, 2011 and effectively replaces SAS 70 as the authoritative guidance for reporting on service organizations. SSAE 16 was drafted with the intention and purpose of updating the US service organization reporting standard so that it mirrors and complies with the new international service organization reporting standard ISAE 3402. This is not a regulation but a standard, and one that gives organizations that adhere to it a badge of quality, which is important in the service industry.

Like SOX, SSAE 16 does not specify what measures need to be in place, but rather the tools and procedures that facilitate the job of the auditors, demonstrate who was doing what in the database, and automate this process and save costs. SSAE 16 supersedes Statement on Auditing Standards (SAS) No. 70 with the professional guidance on performing the service auditor's examination.

Regulatory Compliance and Security

Compliance does not automatically equate to security. A company may be compliant with a host of regulatory requirements, while its databases remain exposed and vulnerable. There are several reasons why this happens:

- Regulations are limited in scope to whatever they are intended to regulate. PCI DSS, for example, is concerned with credit card details and credit card details only. If someone stole your employee data, for instance, this would be of no concern to the PCI auditors.
- Compliance is often audit-focused and audits are, by nature, activities that take place after the fact. So, while you may discover that you had been breached four months earlier, it won't do you much good in reversing that data theft.
- The requirements posed by some regulations represent a minimum baseline not a best practice. They are deliberately created this way to allow many organizations to comply.
- Regulations are outdated as soon as they are published. The threat landscape changes faster than lawmakers write laws and regulators issue regulations.

Reconciling compliance and security requirements

Regulatory compliance can be seen as a burden, or it can be seen as a chance to streamline business processes and significantly upgrade security. To make the best of this opportunity, enterprises should align their compliance projects with security requirements to ensure that the required measures are implemented in one fell swoop.

The big picture

One can easily be preoccupied with the pressing requirements of regulatory compliance and put aside other considerations until those requirements are met. However, enterprises often have multiple compliance requirements to consider, as well as a number of security considerations. Given the great overlap between the different requirements, it would be a waste of resources to go through separate efforts for each objective.

It is useful to take a step back and look at the big picture. Even if your current initiative does not cover all corporate databases, it makes sense to apply all relevant security improvements to those databases touched on by the next audit or compliance project.

Take, for example, a publicly traded healthcare insurance company. It will not only need to comply with Sarbanes-Oxley, but also with HIPAA, privacy notification laws, such as SB 1386, and possibly PCI DSS if the company takes payment by credit card. Many databases would be relevant to two or more regulatory audits, so it is important to map those as in the following example:

Figure 1. Compliance regulations affecting databases, per Industry.

The relevant databases can then be mapped for relevant sensitive data, privileged users, and the type and frequency of audit reports that are required. The additional effort is marginal and provides a more efficient and comprehensive view.

Overlapping requirements

Virtually all compliance requirements adhere to principles that are useful for improving security as a whole, and those can be leveraged for upgrading database security with no additional effort:

- *Controlling access to sensitive data*—Requires identifying sensitive data and using user authentication and monitoring to enforce access policy to that data
- *Separation of duties*—Requires that the people in charge of auditing or monitoring the database are not the same people whose actions are being monitored
- *Monitoring privileged users*—Due to the level of access given to privileged users, such as database administrators, system administrators, and developers, special attention to these transactions is required

Five Principles of Database Protection

1. Think security in everything you do

Constantly examine your actions through a strong security filter. Start with application development, and then move through everyday tasks like user management and data management. In most IT environments, the database landscape changes on a regular basis with the addition of new database instances within both test and production environments. Given the dynamic nature of this landscape, it is critical to maintain maximum visibility into the number, location, sensitivity, and security posture of each and every database. This can be achieved via regular, deep database vulnerability scans, which will discover new databases and identify obvious, easy-to-remediate vulnerabilities that often go undetected due to lack of awareness and process. You must ultimately think of database security as an ongoing process, that with the right dedicated solution can be automated and optimized.

2. Use the least privilege principle

The least privilege principle calls for users and applications to have the minimal privileges they require to function properly. This entails applying restrictions when first granting users access to the database and reviewing access privileges periodically. Some organizations grant deep privileges to temporary workers but forget to remove or change privileges when the work is done. Even seemingly innocent view privileges can be used by some attack vectors to gain access privileges through vulnerabilities, so consider need versus risk before granting privileges.

3. Minimize the attack surface

It is more difficult to secure a large house with many windows than a small house with few windows. Database systems are the same: the more complex they are, the larger the attack surface. Strive to reduce the attack surface, either by eliminating components that are not in use or by simply not installing them in the first place.

4. Encrypt, but not as a panacea

Encryption is often the first thing that comes to mind when securing data, and it is certainly recommended for sensitive data. However, it can be expensive, difficult to use, and difficult to manage in a way that is secure. Encrypt only sensitive data that requires it, be careful how you manage the encryption/decryption keys, and change them on a regular basis.

It is important to combine encryption with other means and procedures, such as activity monitoring, auditing, periodic vulnerability assessments, and user authentication.

5. Development, testing, and staging environments

Many organizations invest efforts in securing their production databases but neglect to do so in development, testing, and staging environments. As the staging environment is often copied into production when it is ready, it should be as secure as the production version. Beyond that, it is often the case that real production data is used in non-production environments without any masking. This poses a serious security risk. It is recommended that non-production environments are treated with the same tools and procedures one as production environments.

Five Practical First Steps

The following are steps that anyone can perform on their database without getting into lengthy projects, vulnerability assessments or the use of expensive tools and third-party services. All they require is a minimal investment of time and attention. These steps will not make your database 100 percent secure, but they will bring you a long way towards a more secure environment.

1. Usernames and passwords

While on trial for multiple counts of data theft, a hacker told the jury in his trial that 80 percent of his successful break-ins were due to weak username and password combinations or the use of standard passwords. This demonstrates that duping the user authentication mechanism is still the easiest way of penetrating a database and nothing makes that easier than sloppy use of default usernames and passwords, weak passwords, and shared passwords.

Oracle and other databases come with built-in default usernames and passwords—several hundreds of them—created to make it easier to set up the system. These should be erased after the system has been set up. There are free tools available on http://www.petefinnigan.com that do just that for Oracle specifically.

Weak passwords are widely regarded as a massive problem within the realm of IT security and include those that are short (fewer that six characters), based on dictionary words or names, and dates. There are tools available for download from the web that can crunch through hundreds of thousands of passwords per minute. These types of tools can go through all of the words in the *Oxford English Dictionary* in less than 30 seconds. Even by using inflections and combinations of words and numbers, such a tool will break through in a very short period of time. It is imperative to use strong passwords that contain a combination of letters, numbers, and symbols.

2. Remove unnecessary components

Database management systems (DBMSs) today, especially enterprise versions, are behemoth applications with many options that most people will seldom use. Certain database vulnerabilities exploit such add-ons and extensions (for example, Oracle APEX). This multitude of components creates a very large attack surface (see the above principles) and thus more opportunities to infiltrate the database. Review your database configuration periodically and remove components—including various extensions and add-ons—that your users are not using. Don't install components until they are really needed.

3. Apply security patches

New database vulnerabilities are uncovered constantly and many are patched by the database vendors themselves, who issue updates and patches to the DBMS. It is not always easy to apply those patches, because they require testing and database downtime. But even deciding on a schedule where patches are applied twice a year is better than not applying them at all.

Ironically, it is precisely when patches are issued by the DBMS vendor that unpatched systems are even more vulnerable to attack. Why? Because the public announcement of the availability of such patches also alerts potential intruders to the existence of vulnerabilities in specific modules.

An alternative and complementary approach is to use virtual patching tools, such as the ones available from McAfee. Those tools create an external layer of defense on top of the database that specifically addresses vulnerabilities and issues alerts or takes action to stop attempts to exploit them.

4. Secure coding practices

Many database vulnerabilities are exposed due to the way applications are coded and their interaction with the database. Lack of accountability and lack of secure coding practices may open the floodgates to breaches and attacks. For example, SQL injections in web applications can be thwarted entirely by binding variables in SQL statements. Unfortunately, many developers still do not use the bind variables method when developing applications, leaving the database exposed to SQL injections.

Architecting and designing for security, validating input, and sanitizing data sent to other systems are some of the recommended methods used in secure coding. You can visit the Computer Emergency Readiness Team (CERT) website for additional information on coding standards.

5. Monitor, audit, monitor, and audit again

You cannot protect an asset if you can't see it or don't know that it even exists. This seems obvious, and yet most database administrators and security professionals have no idea of the exact number, location, data sensitivity, and security posture of each and every database that exists within the environment. This is a massive challenge in environments with thousands of databases—without the proper tools.

Auditing is an offline endeavor that looks back at the database activity over a period. Full native DBMS auditing is impractical, as it significantly slows performance, but selective fine-grained auditing can be used. While certain compliance requirements may force you to audit "everything" and keep an infinite audit trail, it is also impractical—the more benign actions you record, the less likely you are to notice the conspicuous ones. Try and work with the auditors to define the types of activities that are crucial (accessing sensitive data, privileged user access, and others), and record those.

Monitoring occurs in real time and is more actionable and useful in security terms. There are tools, most rather expensive, that are available for enterprise deployments. Some of these tools have prevention capabilities. But now there is a breakthrough product that can monitor multiple databases, terminate attacks by using policy violations as a tool, provide access to virtual patches that protect systems from many known and zero-day vulnerabilities, and deliver real-time notification through email or SIEM/SEM integration.

McAfee Database Activity Monitoring for Real-Time Activity Monitoring and Threat Prevention

McAfee® Database Activity Monitoring is a non-intrusive, activity monitoring sensor that monitors all database activity in real time and can act based on defined rules and policies. It issues alerts on suspicious activity and, if necessary, intervenes in real time. It can also generate activity reports to satisfy auditor requirements.

McAfee Database Activity Monitoring makes use of small footprint sensors in the form of software agents that are installed on the database host server itself and that monitor all activity. The design is non-intrusive, easy to install, and consumes only small amounts of CPU resources (less than 5 percent of one single CPU core). The sensors communicate with the McAfee Database Activity Monitoring server, which generates alerts in accordance with its defined rules. McAfee Virtual Patching for Databases, which leverages this same sensor architecture, offers out-of-the-box protection against known vulnerabilities, and allows for immediate security updates when new vulnerabilities are discovered. This provides a means of patching databases —even ones no longer supported by the DMBS vendor—without significant downtime. Additionally, McAfee Vulnerability Manager for Databases can perform comprehensive scans and identify a wide spectrum of security weaknesses against which the database can be hardened.

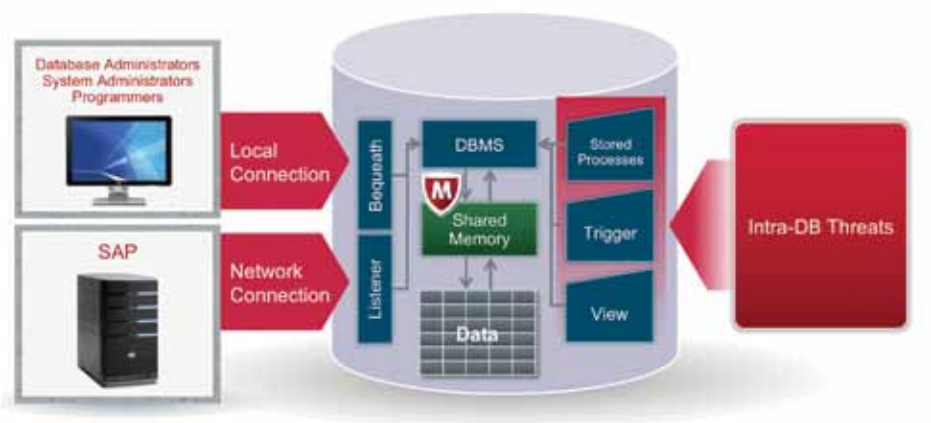

Figure 2. The memory-based McAfee Database Activity Monitoring sensor sees database transactions originating from any of the three main vectors.

The McAfee Database Activity Monitoring policy rules apply to types of SQL statements, database objects accessed, time of day or day of the month, specific user profiles, IP addresses, and the applications used, among other parameters.

The action taken when the conditions of a rule are met can be as simple as logging an event, sending an alert to a SIM/SEM system via email or SMS, or terminating a user session to prevent malicious activity. Users can also be quarantined to prevent subsequent attempts at breaching the database. The system comes with predefined rules that prevent known attacks that exploit database vulnerabilities. McAfee Database Security integrates with McAfee Enterprise Security Manager, a product of the recently acquired NitroSecurity, to further strengthen monitoring and threat prevention capabilities.

A single McAfee Database Activity Monitoring server can manage and communicate with numerous sensors on different databases, and an enterprise installation can scale to support the monitoring of hundreds of databases. The server also easily integrates with IT infrastructure to facilitate central IT management and security event management.

Since the McAfee Database Activity Monitoring sensor is installed on the database machine, it is impossible to bypass and possesses self-defense mechanisms that send out an alert if any tampering attempts are undertaken. The structure of the system ensures separation of duties, with definable roles and access rights to different users.

McAfee employs a "red team," a group of ethical hackers who research new database vulnerabilities. As soon as such vulnerabilities are discovered, the team creates rules that protect against them, acting essentially as virtual patches that immediately protect the database without the need for a system upgrade or downtime. As a result, the database is not exposed and is protected until DBMS updates are issued by the vendor and can be applied as a patch update.

Unique Advantages

The only software-only database monitoring technology that monitors all database activities and provides protection against insiders with privileged access:

- Granular monitoring of database transactions, queries, objects, and stored procedures, with real-time alerts and prevention of breaches
- Flexible rules that allow enforcement of corporate security policy with minimal false positive alerts
- Virtual patching of newly discovered database vulnerabilities, providing immediate protection with no DBMS downtime
- Flexible audit and reporting capabilities suitable for PCI DSS, SOX, and HIPAA
- Highly scalable software solution that is easily deployed across both physical and virtual environments
- Multiple user rules that facilitate separation of duties

McAfee Database Activity Monitoring, McAfee Vulnerability Manager for Databases, and McAfee Virtual Patching for Databases are available for free 30-day trial evaluation, and are downloadable from www.mcafee.com/dbsecurity.

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

McAfee
An Intel Company

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

50002wp_db-compliance_0912_fnl_ASD