Business Brief

Top Five Reasons to Deploy a Dedicated Database Security Solution

Establish a critical last line of defense

Protecting the valuable and confidential information stored within databases is vital for maintaining the integrity and reputation of organizations everywhere—not to mention ensuring regulatory compliance. However, many organizations still rely on security solutions with inherent limitations. Given the complexities of today's database platforms and the sophistication of today's cybercriminals, deploying a comprehensive and dedicated database security solution is a must. Here are five reasons why.

1. You Can't Protect an Asset If You Don't Know It Exists

Even in buttoned-down enterprise IT environments, it's not at all uncommon for there to be hundreds or even thousands of database instances containing highly sensitive information—and IT departments would be hard pressed to come up with the exact number, location, data sensitivity, and security posture of those databases. The worst part is that cybercriminals know this and are always testing for blind spots. They have the time and technical resources to exploit databases you thought were secure or didn't even know existed in the first place. Your lack of visibility is their opportunity.

Complete visibility into your database landscape can only come when you have the ability to perform a full discovery of all existing databases within your environment, along with a scan to identify which of those contain payment card information, human resources data, sales figures, and other sensitive data. In addition, automated, in-depth database vulnerability testing is critical to determining the exact nature of your risks. Only a dedicated database security solution can give you the detailed, actionable information that can prioritize and remediate security gaps, while saving your organization the considerable expense of an outside security consultant.

McAfee® Vulnerability Manager for Databases automatically discovers all databases on your network, determines if the latest patches have been applied, and scans for vulnerabilities. In fact, McAfee Vulnerability Manager conducts more than 4,200 vulnerability checks against leading database systems and classifies threats into distinct priority levels, while providing fix scripts as well as recommendations. It requires minimal knowledge of database systems, generates customized reports in easy-to-understand formats for various user roles, and does it all from a centralized security console.

2. Perimeter Security Doesn't Defend against Insider Threats

You've invested a great deal of time, effort, and capital to select and deploy firewalls and other network security technologies. However, as you know, not all database breaches originate outside the perimeter. In fact, annual research by the Computer Emergency Response Team (CERT) indicates that up to half of database breaches are caused by internal users. So, you need to protect your business-critical data from even more insidious foes—privileged insiders, many of whom have the wherewithal to bypass native database management systems' (DBMS) security features, tamper with access logs, and cover their tracks.

McAfee Vulnerability Manager Advantages

- Gain full visibility into database security posture
- Scan multiple databases across the enterprise from a centralized console
- Accelerate time to compliance and minimize audit cycles, resulting in significant cost savings
- Deploy quickly with minimal database system knowledge
- Quickly generate custom reports in an easy-to-understand format for various user roles

McAfee Database Activity Monitoring Advantages

- Maximize visibility and protection from all sources of attacks
- Monitor external threats, privileged insiders, and sophisticated threats from within the database
- Minimize risk and liability by stopping attacks before they cause damage
- Save time and money with faster deployment and a more efficient architecture
- Achieve flexibility to easily deploy on the IT infrastructure you choose

The right database security solution will detect and prevent threats across all possible vectors: threats originating from the outside and especially from the inside. Furthermore, it will provide a framework for easily setting up and enforcing database access policies in accordance with specific compliance requirements to continuously ensure true segregation of duties.

McAfee Database Activity Monitoring 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. With McAfee Database Activity Monitoring, you gain visibility into all database activity, including local privileged access and sophisticated attacks from within the database. It protects your data from all threats by monitoring activity locally on each database server regardless of location and by sending alerts or automatically terminating sessions that are suspicious or violate security policy in any way. McAfee Database Activity Monitoring even secures your databases and enforces your policies in virtualized or cloud computing environments.

3. The Bad Guys Can Attack Faster Than You Can Patch

Patch Tuesday ought to be declared a holiday for hackers. It's the day of the month when database vendors reveal the ripest targets. What's more, Patch Tuesday gives bad guys a heads up because they know how painful it is for your database management team to take down, patch, and test your databases. In fact, they count on the patching process to be thought of as such an operational disruption that you'll choose to delay it for as long as possible, giving them ample time to find a way in.

There's really no way around the traditional patching process—and the opening it gives to criminals—unless you have a dedicated database security solution. And that solution must enable you to update the security posture of your databases in real time—without making your staff miserable and without disrupting your business operations.

McAfee Virtual Patching for Databases shields databases from the risks associated with unpatched vulnerabilities by detecting and preventing attempted attacks and intrusions in real time, without requiring database downtime or application testing. It gives you peace of mind, since you know that you're protected from threats even during periods of peak vulnerability—the time windows between the issuance of vendor patch updates and actual installation.

McAfee Database Activity Monitoring is another non-intrusive, downtime-free solution that provides an added layer of protection on Patch Tuesday and beyond. Its memory-based sensors intercept attacks on databases coming from across the network, from local users logged into the server itself, and even from inside the database via stored procedures or triggers.

4. You Can't Keep Sacrificing Compliance for Continuity

Regulatory compliance requirements that apply across industries such as healthcare, finance, and retail are constantly evolving and becoming increasingly stringent along the way. Not surprisingly, business-critical databases are heavily impacted by compliance practices, which mandate that databases need to be updated with the latest DBMS vendor-supplied patches. However, given the burdensome nature of having to take down, patch, and then test multiple databases of different types, the majority of organizations sacrifice compliance in order to preserve business continuity. Furthermore, there may be legacy databases still in use for which no patch updates are even offered.

With McAfee Virtual Patching for Databases, you can maintain business continuity without sacrificing regulatory compliance. It allows you to go about your traditional patching efforts on your own schedule, knowing that your databases are secure and compliant. McAfee Virtual Patching for Databases is a tremendous time-saver and a valid compensating control in the eyes of your compliance auditors. In addition, it can even extend the latest protection to legacy databases that are no longer supported by your DBMS vendors.

McAfee Virtual Patching Advantages

- Gain protection from threats even before installing vendor-released patch updates
- Eliminate the need for IT and security teams to have DBMS-specific knowledge
- Keep production databases online, thanks to non-intrusive software design
- Protect databases seamlessly with automatic distribution of ongoing updates
- Facilitate compliance with standards such as PCI DSS, HIPAA, and others

McAfee ePolicy Orchestrator Software Advantages

- End-to-end visibility into database security and compliance from a centralized management console
- A single-pane-of-glass vantage point lets you easily bring databases into a unified security management program, on premises, at remote locations, and even in the cloud
- An open, extensible architecture that connects management of both McAfee and third-party security solutions to your lightweight directory access protocol (LDAP), IT operations, and configuration management tools

5. When Data Lives in the Cloud, Visibility is Extremely Limited

The cloud offers tremendous IT cost and operational advantages but, as you know, there's a catch—your staff can lose control of sensitive data and retain almost zero visibility into who might be accessing it. However, with the right database security solution in place, you can protect your data across both physical and virtual environments. The right solution can prevent unauthorized database activity and can report back to your own management console, even when your database is virtualized and lives in the cloud.

With its unique memory-based sensor implementation, McAfee Database Activity Monitoring can be configured to automatically provision along with each new virtual machine. At the same time, it can request security policies based on the data it hosts, and then begin sending any alerts to the management server. What's more, its sensors can function autonomously even when disconnected from the server, so sensitive data is protected and preserved regardless of whether the database is online or offline or where it resides at any given time. Even if network connectivity is interrupted, data is still protected as the sensor implements the security policy locally and alerts are queued for delivery when the management server is reachable again.

Additionally, access to your cloud-based databases can be monitored via McAfee® ePolicy Orchestrator® (McAfee ePO™) software, which provides an enterprise security management console for end-to-end visibility into database security, enterprise security, and compliance.

In other words, cloud or no cloud, the highest levels of visibility are retained by you and your staff. Clearly, McAfee offers the right database security solution for your IT environment, no matter how widespread your operations are or how sensitive your data might be.

Learn More About Keeping Your Databases Safe and Available

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. It's why we say that safe never sleeps. Rest assured, our team of database security experts is relentlessly focused on keeping your sensitive information safe and available, while helping your company ensure compliance with internal policies and industry regulations.

For more detailed information on how McAfee Database Security can help you protect your business-critical databases, visit www.mcafee.com/dbsecurity, or contact your local McAfee representative or reseller.

Follow us on Twitter: @McAfee_DBSecure.

About McAfee Endpoint Security

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), is the world's largest dedicated security technology company. Our next-generation endpoint security solutions provide security across all of your devices, the data that runs through them, and applications that run on them. These comprehensive and tailored solutions reduce complexity to achieve multilayer endpoint defense—without impacting productivity. It's the perfect blend of traditional smart malware scanning, dynamic whitelisting, behavioral zero-day intrusion prevention, unified management, and integrated threat intelligence. Find out more at www.mcafee.com/endpoint.

McAfee Database Security Advantages

- Deploy and use with ease
- Gain full visibility into your database security posture
- Align security policy administration practices across security and database management personnel
- Efficiently maintain regulatory compliance
- Minimize risk and liability by stopping attacks before they cause damage
- Manage database security from a centralized console

McAfee
An Intel Company

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