McAfee Database Activity Monitoring

Cost-effective database protection to meet your compliance requirements

Organizations store their most valuable and sensitive data in a database, but perimeter protection and basic security provided with the database don't protect you from today's sophisticated hackers or potential threats from rogue insiders. Research[1] shows that more than 96% of records breached involved a database, and 66% of breaches remain undiscovered for several months or longer. McAfee® Database Activity Monitoring—part of the Intel® Security product offering—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. Now it's easier to demonstrate compliance to auditors and improving protection of critical data assets.

Key Advantages

- Maximizes visibility and protection from all sources of attacks.
- Monitors external threats, privileged insiders, and sophisticated threats from within the database.
- Minimizes risk and liability by stopping attacks before they cause damage.
- Saves time and money with faster deployment and a more efficient architecture.
- Gives you the flexibility to easily deploy on the IT infrastructure you choose.
- Integrates with core McAfee products, such as the McAfee® ePolicy Orchestrator® (McAfee ePO™) management platform and McAfee Vulnerability Manager for Databases.

With McAfee Database Activity Monitoring, organizations gain visibility into all database activity, including local privileged access and sophisticated attacks from within the database. McAfee Database Activity Monitoring helps them protect their most valuable and sensitive data from external threats and malicious insiders. In addition to providing a reliable audit trail, McAfee Database Activity Monitoring also prevents intrusion by terminating sessions that violate security policy.

With McAfee Database Activity Monitoring organizations can:

- Quickly build a custom security policy to meet industry regulations or internal IT governance standards.
- Log access to sensitive data for audit purposes, including complete transaction details.
- Terminate sessions violating policies and quarantine suspicious users, preventing data from being compromised.
- Maintain separation of duties as required by many regulations.

McAfee Database Activity Monitoring cost effectively protects your data from all threats by monitoring activity locally on each database server and by alerting or terminating malicious behavior in real time, even when running in virtualized or cloud computing environments.

Protection from All Database Threat Vectors

Attacks targeting valuable data stored in databases can come from across the network, from local users logged into the server itself, and even from inside the database itself via stored procedures or triggers. McAfee Database Activity Monitoring uses memory-based sensors to catch all three types of threats with a single, non-intrusive solution. This information can then be used to demonstrate compliance for audit purposes and to improve security overall for an organization's most valuable data.

Identify Threats as They Occur, Reducing Risk and Liability

Unlike basic auditing or log analysis, which only tell you what happened after the fact, real-time monitoring and intrusion prevention capabilities

stop breaches before they cause damage. Alerts are sent directly to the monitoring dashboard with full details of the policy violation for remediation purposes. High-risk violations can be configured to automatically terminate suspicious sessions and quarantine malicious users, allowing time for the security team to investigate the intrusion.

Virtual Patching Protects from Known Exploits and Many Zero-Day Threats

It's not always possible to install vendor patches immediately, as they often require applications testing and downtime to apply the update. And some applications still use older releases of the databases for which patches are no longer provided. McAfee Database Activity Monitoring detects attacks attempting to exploit known vulnerabilities as well as common threat vectors and can be configured to either issue an alert or terminate the session in real time. 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.

Deploy Quickly and Nonintrusively with Minimal Resources

A software-only solution, McAfee Database Activity Monitoring can be implemented and begin protecting databases in under one hour, without the need for special hardware or additional servers. Further accelerating deployment, McAfee Database Activity Monitoring automatically scans the network for databases and uses wizard-driven templates for various regulatory environments to guide the user in quickly creating custom security policies to meet audit requirements. By distributing the responsibility for implementing security policy to autonomous sensors running on each database server, McAfee Database Activity Monitoring scales cost effectively to support the largest enterprises.

Supports Today's Modern IT Infrastructure, Including Virtualization and the Cloud

Other systems for database monitoring rely on analysis of network traffic to identify policy violations, something that is either impossible or inefficient in the highly dynamic and distributed architectures used for data center virtualization and cloud computing. In contrast, our sensors can be configured to automatically provision along with each new database, request the security policy based on the data it hosts, and then begin sending any alerts to the management server. 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.

Integration with the McAfee ePolicy Orchestrator Platform

McAfee Database Activity Monitor is fully integrated with McAfee ePolicy Orchestrator software, providing centralized reporting and summary information for all your databases from a consolidated dashboard. McAfee ePO software connects with additional McAfee security solutions outside of database protection to provide a single pane-of-glass view for ease of management and complete visibility.

McAfee Database Security Solutions

We offer a number of database security solutions to help you gain complete visibility into your overall database landscape and security posture. To learn more, visit **www.mcafee.com/dbsecurity**, or contact your local McAfee representative or reseller near you.

1. *Verizon Business Study*, 2013.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com