McAfee
An Intel Company

McAfee Database Event Monitor for SIEM

Gain visibility into database transactions without impacting performance

Reliable auditing of database transactions is mandatory for compliance, but traditional native database auditing solutions can cripple database performance and database administrator productivity. The non-intrusive design of McAfee® Database Event Monitor for SIEM supports your expanding compliance auditing and reporting requirements and enhances security operations.

Key Advantages

- Uses passive network-based monitoring for zero impact on database performance
- Discovers all database instances, including unauthorized or rogue databases
- Allows monitoring and logging of access to databases with regulated information
- Retains details of all database transactions from login to logoff to support auditing
- Simplifies analysis with "one click" reconstruction of sessions
- Fully integrated with McAfee Enterprise Security Manager to enable database transactions to be used in event correlation and other advanced SIEM activities
- Flexible, hybrid delivery options include physical and virtual appliances

McAfee Database Event Monitor for SIEM delivers non-intrusive, detailed security logging of databases and applications, monitoring all access to sensitive corporate and customer data. With minimal deployment effort, you can have visibility into database transactions, events, and specific database queries and responses—including who is accessing your data and why.

McAfee Database Event Monitor for SIEM is the only product of its kind that both consolidates database activity into a central audit repository and provides normalization, correlation, analysis, and reporting of that activity.

Predefined rules and reports and privacy-friendly logging features make it easy to comply with compliance regulations while strengthening your overall security posture.

Database Access in Context

Going far beyond logging, McAfee Database Event Monitor for SIEM normalizes data and correlates database transactions with other information to help you perform real-time analysis.

By expanding visibility to include user information, application content, operating system activity, vulnerabilities, and even network location, McAfee Database Event Monitor for SIEM allows you to:

- Track users across applications
- Examine full session activity, from login to logoff
- Detect sensitive data and identify policy violations
- Detect loss of data through authorized channels
- Correlate database activity to security events
- Produce an audit trail of all database activity
- Generate detailed reports for PCI-DSS, HIPAA, NERC-CIP, FISMA, GLBA, SOX, and many more

Full Visibility into Each Transaction

McAfee Database Event Monitor for SIEM monitors all database transactions and provides a complete audit trail of all database activities, including queries, results, authentication activity, and privilege escalations. Since McAfee Database Event Monitor for SIEM maintains full session details of all transactions, you can easily see what happened before and after any given transaction—from login to logout.

Automated Compliance Processes

Pre-built policy-based detection rules and compliance reports ensure that you can generate the data access information required by PCI-DSS, HIPAA, NERC-CIP, FISMA, GLBA, SOX, and others. In addition, McAfee Database Event Monitor for SIEM fully integrates with McAfee Enterprise Security Manager and McAfee Enterprise Log Manager for unprecedented event analysis and correlation in addition to compliant storage and masking of sensitive data in activity logs.

An exception list shows database servers not being monitored as well as illegal ports opened to access data from databases.

User and Account Tracking

Using the advanced capabilities of the McAfee Security Management product line, users and administrators can easily be tracked across multiple applications, and accounts, providing end-to-end accountability of all user activity, regardless of how they accessed the database.

User Activity Profiling

McAfee DEM tokenizes every SQL query into commands— objects (tables, views, stored procedures) being accessed on target database servers while generating a profile of each users behavior, revealing both new and abnormal activity.

Database monitoring functions

- Monitor and log all database activity
- Support compliance efforts
- Deter eavesdropping
- Increase accountability
- Alert on objects, actions, and policy violations
- Capture valuable metrics for database service level/ performance management
- Monitor all paths to data, including:
  - Applications
  - Users
  - Malware
  - Utilities
  - Back-doors
  - Queries
  - LAMP scripting
  - Open Database Connectivity (ODBC)

SQL Injection

All SQL query response packets are monitored for query success and failure. Low severity failures such as syntax errors, which are symptomatic of a SQL injection attack, are tracked and correlated if they happen in succession—a guaranteed way of proactively detecting SQL injection attempts.

Risk and Threat Detection

McAfee Database Event Monitor for SIEM analyzes all monitored activity against a customizable set of policy rules and detects and alerts on all suspicious activity. In addition, anomaly-based detection indicates abnormal user activity, queries, responses, and other out-of-place behavior.

Power Without the Overhead

McAfee Database Event Monitor for SIEM appliances, featuring a high-performance data capture engine, monitor your database over the network—imposing no overhead on the database itself and ensuring the audit data you need is retained.

McAfee Enterprise Security Manager provides management and connects database monitoring with the rest of your security and compliance ecosystem. To add visibility into local terminal activity, use an optional host agent, which delivers a lower performance impact than competing host agents or native auditing.

Use Cases

Compliance

To help you ensure compliance, McAfee Database Event Monitor for SIEM can discover sensitive data in use. You can monitor these databases and establish an audit trail for protected data access, user account activity, and changes. Security duties can be segregated from database administration for tighter control, and sensitive data can be masked from logging. Reports can highlight top consumers of protected records. Pre-built reports for different regulations can be generated at any time.

Database detection and classification

By monitoring the network for database commands, McAfee Database Event Monitor for SIEM is able to detect all database instances—including unknown or rogue databases. In addition, McAfee Database Event Monitor for SIEM monitors all transactions, including query results, and analyzes them against policy rules and dictionaries to detect which databases are storing credit cards, social security numbers, or other sensitive data.

Security monitoring

McAfee Database Event Monitor for SIEM monitors your databases directly and can detect and alert you in real time to brute-force logins, SQL injection attacks, abnormal access patterns, and other indications that your database server might have been breached. You can monitor back-end application activity and detect suspicious activity, including fraudulent data retrieval and rogue user accounts.

If the attack originated from within the network, you can track user activity and correlate against network flow data to identify and locate the offender. In the case of an outside attack, the breach can be correlated against other outbound network and application activity to discover data loss, covert communications channels, and other loss vectors.

System Specifications

Hardware Specifications	DSM-4600	DSM-3450	DSM-2600
Collection Rates	15,000 events per second	10,000 events per second	5,000 events per second
Interfaces	8 x 10/100/1000 Mbps Ethernet copper interfaces	4 x 10/100/1000 Mbps Ethernet copper interfaces	4 x 10/100/1000 Mbps Ethernet copper interfaces

For more information, visit mcafee.com/DEM.

McAfee
An Intel Company

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

50103ds_db-event-monitor_0812_fnl