Product Datasheet

dbDefender™ for DB2, McAfee DAM Agent Version

CorreLog dbDefender™ for DB2 — certified DAM agent for McAfee Data Center Security Suite

The sophistication of malicious hackers today warrants that your perimeter defense strategy become much more than just log management and event correlation. Considering that 80 percent of the world's corporate data resides on mainframes, we must consider user activity on mainframes as a daily staple of Security Information and Event Management (SIEM) strategies. SIEM solutions however, are essentially Windows- and UNIX-based and an information gap has been wedged between these systems and mainframe systems such as IBM z/OS.

Within IBM z/OS, DB2 has become the enterprise server standard for data management for the massive workloads executed on mainframes. From an enterprise security perspective however, there needs to be a live connection from DB2 to your distributed SIEM system and an audit trail for this wide-scale access to DB2. This is a function that is called Database Activity Monitoring (DAM). CorreLog has partnered with McAfee who is leveraging the CorreLog DAM Agent, dbDefender™, to provide a live feed of user event monitoring on DB2 to McAfee DAM.

CorreLog dbDefender™ delivers up-to-the-second security alerts to McAfee DAM on DB2 accesses, change, inserts, transactions, table activity and more. McAfee DAM users now have visibility provided by the dbDefender™ Agent that includes a host of user events centered around attempts to alter the secure state of DB2.

Security admins using McAfee DAM with dbDefender™ no longer have to wait for a nightly or weekly batch report for DAM auditing. McAfee DAM with dbDefender™ also delivers real-time DB2 monitoring and alert messaging. Any organization with PCI DSS or other industry standard requirements needs this up-to-the-second monitoring of DB2 to ensure compliance while minimizing risk. Specifically, McAfee DAM powered by dbDefender™ provides the following DAM capability:

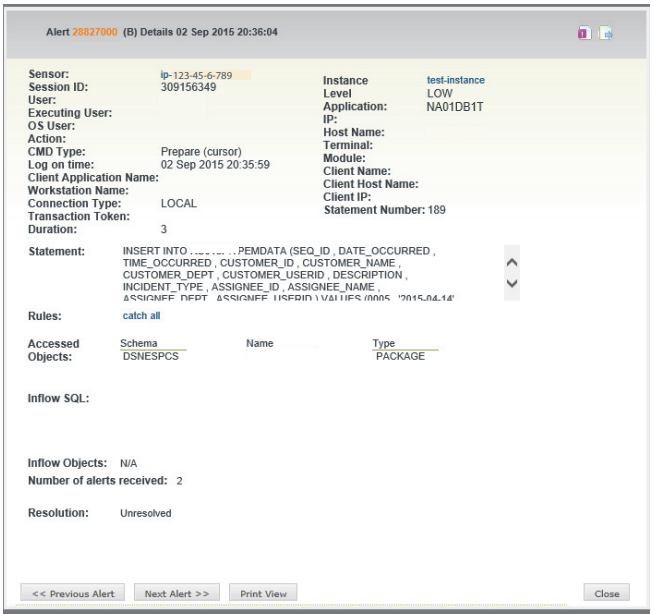
- **Privileged user activity monitoring**
- **Auditing invalid logical access attempts**
- **Auditing creation and deletion of system-level objects**
- **Additional auditing of DB2 Utilities, DDL statements, DB2 console commands, DB2 object access, and other user activity linked to DB2**
- **Detailed monitoring down to SQL statements**

McAfee DAM, with CorreLog dbDefender™ for DB2, delivers the real-time security events from DB2 accesses that provides the decision-support needed to minimize risk to your mainframe.

CorreLog dbDefender™ for DB2 feeding McAfee DAM, a powerful duo for real-time DB2 security

Practical application of dbDefender™ for DB2, McAfee DAM version, in the field:

FUNCTION	USE CASE
Collects real-time audit events as they take place from DB2	Know who accessed what data and when. Key for PCI DSS, HIPAA, SOX, FISMA, GLBA and other compliance standards
Automated audit trail for all DB2 access activity	Tracks all user and admin DB2 activities, including SELECTs, DML, data definition language (DDL) and changes in access privilege
Audits all valid and invalid attempts to access DB2 data	Tracks invalid logical access attempts and sends to your SIEM system, a critical component for PCI DSS
System-level object create and delete tracking through DB2	Another PCI DSS standard covered, an audit trail for DB2 data structure changes
Audits critical table writes and reads to DB2	DAM function that facilitates PCI DSS standard 10.2 - the logging of all access to credit cardholder data
Leverages instrumentation facility interface (IFI) for querying of DB2 data	More efficient approach for collecting DB2 events for Syslog conversion, reducing system overhead
Supports both static and dynamic SQL	Capable of "watching" both embedded SQL and SQL using APIs
Supports wide range of VSAM file types	Capable of tracking access to sequenced dataset (ESDS), key-sequenced data set (KSDS), relative record data set (RRDS), virtual relative record data set (VRRDS) and linear data set (LDS), monitoring OPENs, READs, UPDATEs, DELETEs, CREATEs and ALTERs



DB2 alerts from CorreLog dbDefender™ for DB2

For more information on CorreLog dbDefender™ for DB2, McAfee DAM version, please visit www.CorreLog.com.

About CorreLog, Inc.

CorreLog, Inc. is the leading independent software vendor (ISV) for IT security log management and event correlation spanning both distributed and mainframe platforms. CorreLog's flagship products are zDefender™ for z/OS, zDefender™ Visualizer for z/OS, and dbDefender™ for DB2, and CorreLog SIEM Correlation Server.

CorreLog, Inc.
Naples, FL
1-877-CorreLog | +1-239-514-3331
www.CorreLog.com | info@CorreLog.com