

BMC AMI Defender for Db2

Real-Time Database Activity Monitoring for Db2

The sophistication of malicious hackers today warrants that your perimeter defense strategy become much more than the status quo. You must have real-time user event data from every corner of your enterprise, including your mainframe. Eighty percent of the world’s corporate data resides on mainframes; the WIN/UNIX security-only approach is slowly becoming a perimeter defense strategy of the past.

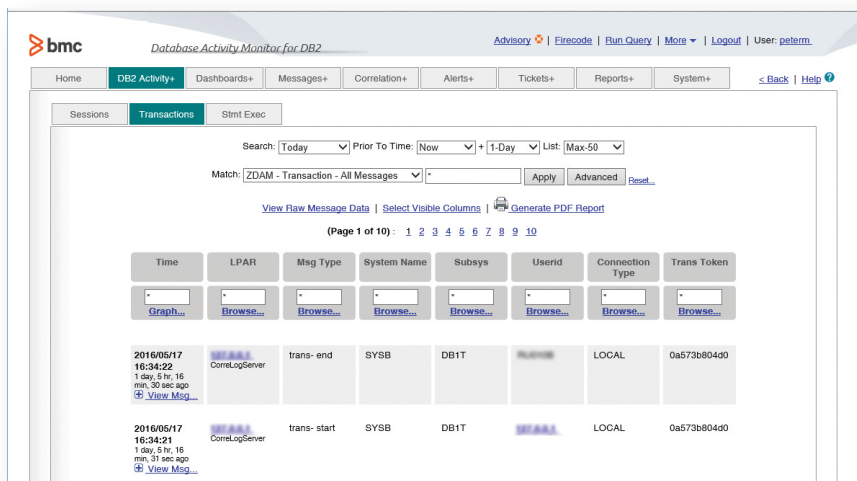
For IBM z/OS, Db2 has become the enterprise server standard for database performance and availability for the massive workloads managed on mainframes. For end-to-end security, your organization needs to include an audit trail for Db2 and that trail starts with a function called Database Activity Monitoring or DAM.

BMC AMI Defender for Db2 delivers up-to-the-second Db2 security alerts to BMC AMI Command Center for Security, BMC Defender SIEM Correlation Server for Windows/UNIX, or any name-brand Security Information & Event Management (SIEM) product. With AMI Defender for Db2, security admins now have up-to-the-second visibility that includes a host of user events centered around attempts to view or access the secure state of your Db2 environment.

HACKERS WANT YOUR DB2 DATA. PROTECT IT WITH BMC AMI DEFENDER FOR DB2:

- The top 25 global banks are on IBM z/OS
- 90% of the top worldwide banks (by assets) are on z/OS
- 23 of the top 25 U.S. retailers are on z/OS
- 21 out of the top 25 insurance organizations are on z/OS
- 9 of the top 10 global life and health insurance providers are on z/OS

Source: IBM presentation from SHARE.org conference 2014





⬆ BMC AMI Defender for Db2 feeding Db2 transactions to BMC AMI Command Center for Security. BMC AMI Defender for Db2 is certified for IBM® QRadar®, HP ArcSight, RSA Security Analytics Solutionary, NetIQ, Micro Focus/Serena and McAfee ESM. We also have field integrations with other leading SIEMs including Splunk, LogRhythm, Dell SecureWorks, and many others.

Any organization needing to adhere to PCI DSS, HIPAA, SOX, IRS Pub. 1075 or other industry standard, needs this real-time Db2 alerting to ensure compliance while minimizing risk. Specifically, BMC AMI Defender for Db2 provides the following DAM capability:

- Privileged user monitoring
- Auditing invalid logical access attempts, changes, inserts, transactions, and table activity
- Auditing 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

Practical application of BMC AMI Defender for Db2 in the field:

 FUNCTION	 USE CASE
<ul style="list-style-type: none"> • Collect real-time audit events as they take place from Db2 	<ul style="list-style-type: none"> • Know who accessed what data and when. Key for PCI DSS, HIPAA, SOX, FISMA, GLBA and other compliance standards
<ul style="list-style-type: none"> • Automated audit trail for all Db2 access activity 	<ul style="list-style-type: none"> • Tracks all user and admin Db2 activities, including Data Manipulation Language (DML), Data Definition Language (DDL) and Data Control Language (DCL)
<ul style="list-style-type: none"> • System-level object create and delete tracking through Db2 	<ul style="list-style-type: none"> • Another PCI DSS standard covered, an audit trail for Db2 data structure changes
<ul style="list-style-type: none"> • Audits critical table writes and reads to Db2 	<ul style="list-style-type: none"> • DAM function that facilitates PCI DSS standard 10.2 — the logging of all access to credit cardholder data
<ul style="list-style-type: none"> • Leverages instrumentation facility interface (IFI) for querying of Db2 data 	<ul style="list-style-type: none"> • More efficient approach for collecting Db2 events for distributed Syslog conversion, reducing system overhead
<ul style="list-style-type: none"> • Supports both static and dynamic SQL 	<ul style="list-style-type: none"> • Capable of “watching” both embedded SQL and SQL using APIs

 **HIGH SECURITY YIELD, LOW COST OF OWNERSHIP**

Few software vendors offer IMS access auditing solutions for the mainframe, and the lack of competition has driven the cost of these solutions sky-high, until now. BMC AMI Defender for Db2 is an affordable and highly-functional, real-time data auditing

product made for mainframe. BMC AMI Defender for Db2 is easy to install and consumes minimal system resources. Contact BMC today at www.bmc.com for a product demonstration.

 **CERTIFIED FOR:**





FOR MORE INFORMATION

For more information on BMC AMI for Security solutions and products, please visit bmc.com/ami-security.

About BMC

BMC helps customers run and reinvent their businesses with open, scalable, and modular solutions to complex IT problems. Bringing both unmatched experience in optimization and limitless passion for innovation to technologies from mainframe to mobile to cloud and beyond, BMC helps more than 10,000 customers worldwide reinvent, grow, and build for the future success of their enterprises.

www.bmc.com



BMC, BMC Software, the BMC logo, and the BMC Software logo, and all other BMC Software product and service names are owned by BMC Software, Inc. and are registered or pending registration in the US Patent and Trademark Office or in the trademark offices of other countries. All other trademarks belong to their respective companies. © Copyright 2018 BMC Software, Inc.

