Product Datasheet

dbDefender™ 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 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.

CorreLog dbDefender™ for DB2 delivers up-to-the-second DB2 security alerts to zDefender™ Visualizer for z/OS, CorreLog SIEM Correlation Server for Windows/UNIX, or any name-brand Security Information & Event Management (SIEM) product. With dbDefender™, 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.

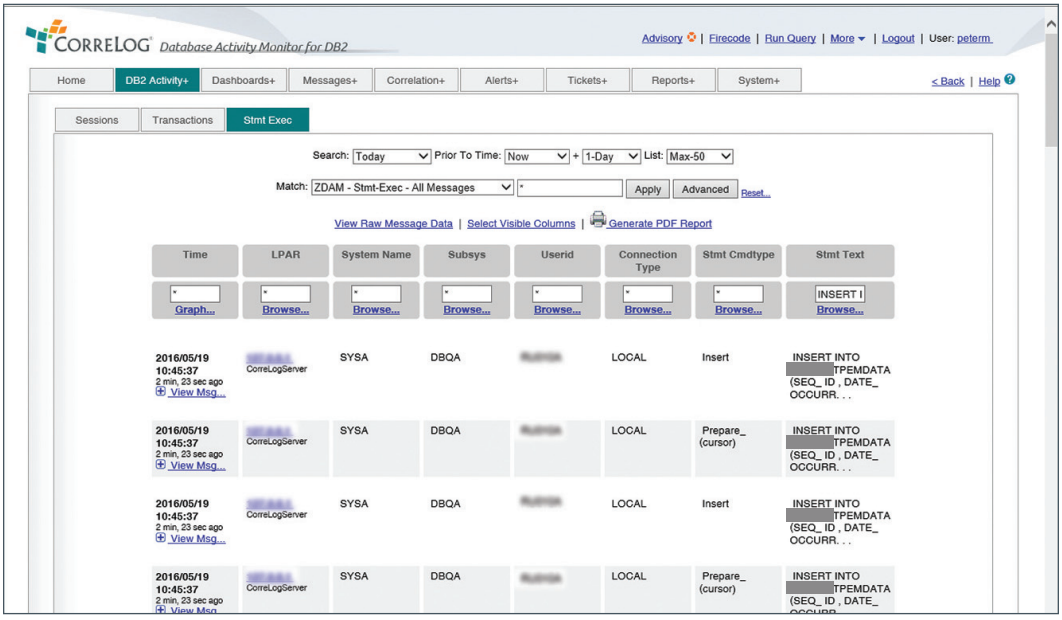
Any organization needing to adhere to PCI DSS, HIPAA, SOX, IRS Pub. 1075 or other industry standard, needs this real-time DB2 alerting to ensure compliance while minimizing risk. Specifically, dbDefender™ provides the following DAM capability:

Hackers want your DB2 data. Protect your data with CorreLog dbDefender™:

- 25 of 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

- 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



CorreLog dbDefender™ feeding DB2 transactions to CorreLog zDefender™ Visualizer for z/OS. dbDefender™ 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.

Practical application of dbDefender™ for DB2 in the field:

Function	Use Case
Collect 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 Data Manipulation Language (DML), Data Definition Language (DDL) and Data Control Language (DCL)
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 distributed Syslog conversion, reducing system overhead
Supports both static and dynamic SQL	Capable of “watching” both embedded SQL and SQL using APIs

High Security Yield, Low Cost of Ownership

Few software vendors offer DAM solutions for the mainframe, and the lack of competition has driven the cost of these solutions sky-high, until now. CorreLog dbDefender™ is an affordable and highly-functional, real-time DAM product made for mainframe. dbDefender™ is easy to install and consumes minimal system resources. Contact CorreLog today at www.correlog.com for a product demonstration.

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 sells software-only solutions that are quick to deploy and complementary to your existing solutions investments.

Certified for:

Business Partner IBM
Ready for Security Intelligence

ArcSight CEF Certified 2016

Technology RSA READY Partner

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