Overview Datasheet

CorreLog Agent for z/OS with dbDefender™ for DB2

CORRELOG®
Proactive Security Correlation & Log Management

Deliver IBM z/OS Data to Your SIEM in Real Time

For many large organizations, one or more IBM z/OS mainframes constitute a strategic capital investment for their most mission-critical applications and processes. The CorreLog Agent for z/OS with dbDefender enables these organizations to combine z/OS SMF events with SIEM Syslog data giving IT security personnel a complete system-wide vantage point for cyber-threat and security breach alerts. With security information and event management (SIEM) software platforms existing predominantly in distributed environments, the CorreLog Agent for z/OS allows organizations to include mainframe event log data for a unified, multi-platform view of enterprise security event data in a single console.

In a concerted effort with SIEM monitoring applications, the CorreLog Agent for z/OS allows the user to view mainframe SMF security, database and TCP/IP events, alongside events from Windows, UNIX, Linux, routers, firewalls, and other IT assets. When included with other log and event data within the CorreLog Server, CorreLog's unique correlation engine and help-desk ticket auto notification feature can alert IT security personnel of cyber-threats before they happen.

The CorreLog z/OS Agent installs quickly, uses minimal resources, and does not require extensive training, ongoing maintenance or administration. CorreLog z/OS Agent is easily configured, allowing users to select from a myriad of events including TSO Logons, Production Job ABENDs, TCP/IP Connections, FTP File Transfers, CA Top Secret, ACF2, RACF and DB2 accesses. Out of this event log data, security systems administrators may filter further by sub-categories and receive only the data relevant to security threats. This filtering capability streamlines data flow to SIEM system consoles without compromising network bandwidth.

The CorreLog z/OS Agent also facilitates increasing compliance regulations such as PCI DSS, FISMA, HIPAA, NERC and Sarbanes-Oxley.

dbDefender for z/OS DB2

The CorreLog Agent for IBM z/OS ships with dbDefender™ which provides real-time monitoring for DB2. Any organization with PCI DSS or other industry standard considerations needs this up-to-the-second data activity monitoring (DAM) of DB2 to ensure compliance. Specifically, dbDefender provides the following DAM capability:

- Privileged user 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.
- dbDefender supports both static and dynamic SQL

Overview Datasheet

CorreLog Agent for z/OS with dbDefender™

SIEM Agent for IBM Mainframes

Feature	Benefit
Standards compliant. Creates RFC 3164-compliant Syslog messages that work with any standards-based SIEM or Syslog collection software	Investment protection. Compatible with all of your existing software. Freedom of choice: select CorreLog or any other Syslog console
Collects events from mainframe security subsystems including RACF® and ACF2	Complements your existing mainframe security software
Collects audit events from DB2	Know who accessed what data and when. Necessary for FISMA, PCI DSS, HIPAA, NERC and Sarbanes-Oxley compliance
Real-time automated audit trail using DB2 IFCID 361	Know how users with root or admin privileges are accessing critical data
Audits invalid access attempts through DB2 IFCID 140	Tracks invalid logical access attempts and sends to SIEM system, a critical component for PCI DSS
System-level object create and delete tracking through DB2 IFCID 97	Another PCI DSS standard is covered here, an audit trail for DB2 data structure changes
Audits critical table writes and reads through DB2 IFCID 143 and IFCID 144	DAM function that facilitates PCI DSS standard 10.2 - the logging of all access to credit cardholder data
Extensive yet straightforward user customization. Decide which events and fields you want to see.	Get the data you need without unnecessary clutter
Works with any version of CorreLog Enterprise Server or any industry-standard SIEM console	Flexibility and investment protection
Collects TSO logons and logoffs	Know who is accessing your system and when. Required for FISMA, PCI DSS, HIPAA, NERC and Sarbanes-Oxley compliance
Collects z/OS job and started task terminations including ABENDs	Know what's working and what's not working in real time in your z/OS production
Audits the use of FTP	FTP is considered by many to be the number one mainframe security exposure. Be alerted to suspicious FTP events in real time
Collects login, telnet and other events from TCP/IP	In the event of an unauthorized access pinpoint the exact source of the threat in real time
Uses only a few seconds of CPU time per day	Thrifty use of mainframe resources. Does not contribute to escalating software costs
Installs in just a couple of hours, not days!	You are up & running, and protected with a very fast turnaround to implementation.
Capacity of hundreds of thousands of Syslog messages per day	No matter what your data volume, CorreLog Agent for z/OS will keep up
Compatible with CorreLog's powerful correlation engine	Correlate related security events from mainframe and Windows®, Linux and UNIX® sources
No impact on existing operations.	No training time, no down time

The following are samples of alert messages reported by the CorreLog Agent for z/OS. These messages were translated from IBM System z SMF data and integrated alongside existing Syslog messages within a client's SIEM system.

Sample ACF2 Violation as reported by CorreLog Agent to a SIEM

MVSSYSB ACF2: EventDesc: Logonid modification - ChgDesc: Change - JobNm: DECR001 - UserID: DECR001 - Pgm: ACF02ALT - Name: Jon User - Rel#: 140 - RdrTime: 2012-07-03T12:13:23.860 - ASID: XE34 - DelTime: 2012-07-03T13:16:49.991 - UID: 0MVSDGRPAAABDECR001 - LogonID: USER02 - LIDuser: {Scty Off, Acctg} - LIDname: SYSADMIN - LIDupdt: 2012-07-03T13:16:49.991 - LIDpwChg: 2012-07-03T13:15:45.688 - LIDmaskDSN: USER02 - New: {CICS: Yes - GROUP: USERGRP}

Sample RACF Violation as reported by CorreLog Agent to a SIEM

MVSSYSB RACF: RESOURCE ACCESS: Insufficient Auth - UserID: TS053A - Group: RESTRICT - Auth: Normal check - Reas: AUDIT option - Job: TS053ATR - Res: SYS1.PROD.PROCLIBT - Req: READ - Allow: NONE - Vol: SYS001 - Type: DATASET - Prof: SYS1.PROD.PROCLIBT - Owner: DATASET - Name: ROBERT SMITH - POE: INTRDR

Sample FTP Client Data

One of your mainframe users accessing an outside host

MVSSYSB TCP/IP: Subtype: FTP client complete - Stack: TCPIP - AS: RX239JB - UserID: RX239JB - SubCmd: RETR - FileType: SEQ - RemtDataIP: ::ffff:23.36.0.209 - RemtID: rx239jb - DStype: Seq - Start: 11037 22:34:33.87 - Dur: 0.00 - Bytes: 6123 - LReply: 250 - Host: MVSSYSB - DSN: RX239JB. ACCOUNT.MASTER - Security: {Mech: None - CtlProt: None - DataProt: None - Login: Undefined}

Sample FTP Server Data

An outside user successfully copying a file from your mainframe

MVSSYSB TCP/IP: Subtype: FTP server complete - Stack: TCPIP - AS: FTPD1 - Op: Retrieve - FileType: SEQ - RemtDataIP: ::ffff:10.31.0.209 - UserID: RX239JB - DStype: HFS - Start: 11037 22:32:45.21 - Dur: 0.78 - Bytes: 56324 - LReply: 250 - SessID: FTPD100335 - DSN: /u/rx239jb/Source/Fields.C - Security: {Mech: None - CtlProt: None - DataProt: None - Login: Password}

Sample FTP Server Logon Failure

An unauthorized user attempting to access your mainframe

MVSSYSB TCP/IP: Subtype: FTP server logon fail - Stack: TCPIP - AS: FTPD1 - UserID: IBMUSER - RemtIP: ::ffff:208.3.0.2 - UserID: IBMUSER - Reas: Password invalid - SessID: FTPD100345 - Security: {Mech: None - CtlProt: None - DataProt: Undefined - Login: Password}

Sample DB2 Audit Data

MVSSYSA DB2: Subsys: D91B - AuthID: DV233B - CorrID: JDBC4DB2 - Plan: DISTSERV - OpID: DV233B - Loc: RS91D91B - NetID: GA0A0707 - LU: C68B - Conn: SERVER - SQL: {Insert: 1 - Prepare: 2 - Open: 1 - Create Table: 7 - Create Index: 9 - Create Tablespace: 7 - Fetch: 1}

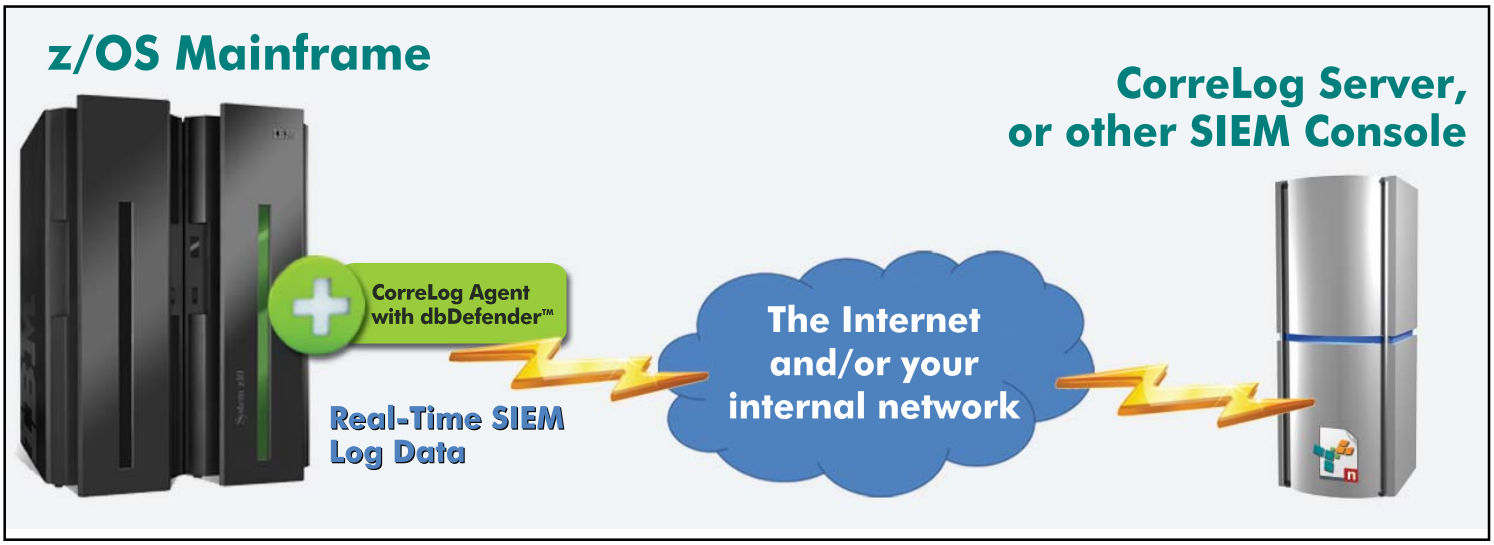
Overview Datasheet

CorreLog Agent for z/OS with dbDefender™

SIEM Agent for IBM Mainframes

IBM z/OS SMF data is an excellent source of event data that can be added to current Syslog data in your SIEM system, expanding your security reach cross-platform and into mainframe environments. With the CorreLog z/OS Agent you have the capability to monitor the following in real-time:

- TSO logons
- Job and STC failures
- Dataset access
- DB2 access records auditing
- CICS transactions
- TN3270 logons, logoffs
- FTP client/server access records
- RACF & ACF2 logs for intrusion and change tracking



The CorreLog IBM z/OS Agent converts SMF messages in real time to Syslog and delivers them directly to your SIEM solution.

Free 30 Day Trial Available for Download

Download CorreLog's Security Correlation Server, Windows Agent, File Integrity Monitor, UNIX/Linux Agent, z/OS Agent and McAfee ePO integration module today for a free 30 day evaluation. These downloads are available at www.correlog.com.

About CorreLog, Inc.

CorreLog, Inc. delivers security information and event management (SIEM) combined with deep correlation functions. CorreLog is real-time, SIEM software that automatically identifies and responds to network attacks, suspicious behavior and policy violations. CorreLog collects, indexes and correlates user activity and event data to pinpoint security threats, allowing organizations to respond quickly to compliance violations, policy breaches, cyber attacks and insider threats. CorreLog provides auditing and forensic capabilities for organizations concerned with meeting SIEM requirements set forth by PCI/DSS, HIPAA, SOX, FISMA, GLBA, NCUA, and others. Maximize the efficiency of existing compliance tools through CorreLog's investigative prowess and detailed, automated compliance reporting. CorreLog markets its solutions directly and through partners. Visit www.correlog.com for more information.

1004 Collier Center Way, Suite 103 · Naples, Florida 34110 · 1-877-CorreLog · 239-514-3331 · info@correlog.com