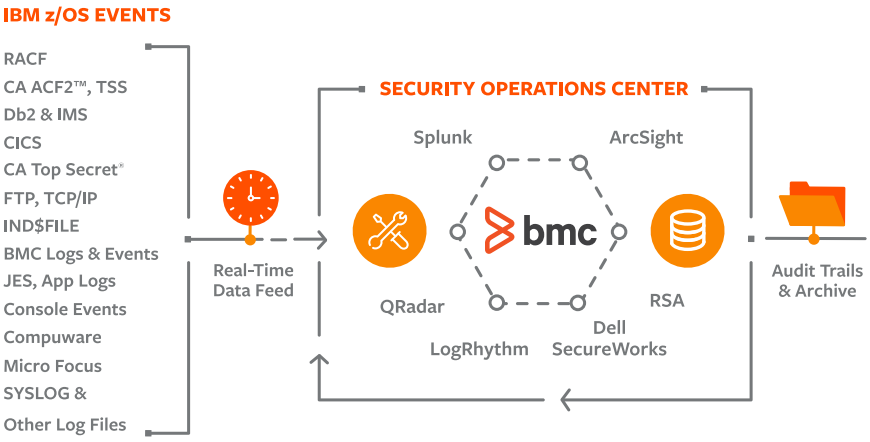
Datasheet

BMC AMI Defender for z/OS

Deliver IBM z/OS RACF, ACF2, & Top Secret User and Db2 Access Data to Your Distributed SIEM in Real Time

For many large organizations, one or more IBM z/OS mainframes constitutes a strategic capital investment for the most mission-critical applications, processes and data. With security information and event management (SIEM) software platforms existing predominantly in distributed environments, the AMI Defender 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.



AMI Defender for z/OS allows users to view mainframe RACF, ACF2, Top Secret, and Db2 events in real-time, alongside security events from Windows, UNIX, Linux, routers, firewalls, and other IT assets in an enterprise SIEM system. This not only provides companies with the best possible security in real-time, but also helps ensure regulatory compliance.

Additionally, AMI Defender converts a myriad of additional mainframe security events including TSO Logons, Production Job ABENDs, TCP/IP and FTP Connections. For ease of deployment, AMI Defender has certified integrations with IBM® Security QRadar®, HP ArcSight, and strategic partnership with Compuware, Micro Focus/ Serena and McAfee. zDefender™ has field integrations with many other leading SIEM solutions including Splunk and LogRhythm. The ability to view cross-platform security event log data in real-time is a ground-breaking feature of AMI Defender.

AMI DEFENDER FOR DB2 OPTION

AMI Defender for z/OS also has an option for real-time Db2 monitoring with AMI Defender for Db2. Any organization with PCI DSS or other industry-standard considerations need this up-to-the-second database activity monitoring (DAM) of Db2 to ensure compliance. Specifically, AMI Defender for Db2 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
- AMI Defender for Db2 supports both static and dynamic SQL

Our real-time z/OS agent provides IT security personnel with a more inclusive view of system-wide threat data for a higher level of monitoring user and system accesses related to network intrusion. AMI Defender facilitates compliance requirements set forth by PCI DSS, HIPAA, IRS Pub. 1075, GLBA, SOX, FISMA, NERC and many other standards.

AMI Defender installs quickly, uses minimal resources, and does not require extensive training, ongoing maintenance or administration. AMI Defender also monitors IBM Db2 utilizing AMI Defender for Db2, which delivers up-to-the-second database activity monitoring (DAM) for Db2. DAM capabilities in BMC AMI Defender for Db2 include privileged-user monitoring, recording invalid access attempts, auditing creation/deletion of system-level objects and other attempts to alter the secure state of Db2, down to the SQL statements.

Your IBM z/OS platform is the most strategic data asset in your enterprise network. It is constantly generating messages that tell you how users and programs are accessing the system, but if you are not receiving these messages in your SIEM in real time, you are putting your data at risk. You can leverage this live mainframe security data within your existing SIEM investment, expanding your IT security visibility outside of your distributed systems. With the AMI Defender, you have the capability to monitor the following mainframe activity in real-time:

- RACF, ACF2, Top Secret messages
- FTP client/server access
- TCP/IP connections
- TSO logons
- Job and started task terminations including ABENDs
- z/OS console messages
- Dataset accesses
- Db2 and IMS accesses
- CICS transactions
- TN3270 logons, logoffs
- Plus other security-related event messages from z/OS

HOW AMI DEFENDER FOR Z/OS WORKS

AMI Defender for z/OS resides in an LPAR (or multiple LPARs) and converts RACF, ACF2, Top Secret and other user data related to mainframe security, and in real time, sends the data as standard RFC 3164 Syslog to your distributed SIEM. The messages leave z/OS ready-formatted for SIEM and no further processing is required. AMI Defender is also compatible with the latest IBM z System, the z14 mainframe.

There are many reasons why AMI Defender for z/OS is the right choice for your Mainframe Security & Compliance initiatives.

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 BMC or any other SIEM system
Collects events from mainframe security subsystems including RACF®, ACF2, and Top Secret	Complements your existing mainframe security software
Collects audit events from Db2	Know who accessed what data and when. Key for PCI DSS, HIPAA, SOX, FISMA, GLBA and other compliance standards
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 your SIEM system, a critical component for PCI DSS
System-level object create and delete tracking through Db2 IFCID 97	Another PCI DSS standard covered, 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

FEATURE	BENEFIT
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 BMC SIEM Correlation Server or any industry-standard SIEM system	Flexibility and investment protection
Collects TSO logons and logoffs	Know who accessed what data and when. Key for PCI DSS, HIPAA, SOX, FISMA, GLBA and other compliance standards
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 system
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
Leverages instrumentation facility interface (IFI) for querying of Db2 data	More efficient approach for collecting Db2 events for Syslog conversion, reducing system overhead
Installs in less than 2 hours. Compatible with IBM z13 system	You are up & running, and protected with a very fast turnaround to implementation
Capacity for millions of Syslog messages per day	No matter what your data volume, AMI Defender for z/OS will keep up
Compatible with the BMC SIEM correlation engine	Correlate related security events from mainframe and Windows®, Linux and UNIX® sources
No impact on existing operations	No training time, no downtime, no maintenance required

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

SAMPLE ACF2 VIOLATION AS REPORTED BY AMI DEFENDER FOR Z/OS TO A SIEM

Feb 18 12:47:32 MVSSYSB ACF2: EventDesc: Logonid modification - ChgDesc: Change - JobNm: SYSRO01 - UserID: SYSRO01 - Pgm: ACF02ALT - Name: ROSS FELLOWS - Rel#: 140 - RdrTime: 2014-02-18T12:13:23.860 - ASID: XE34 - DelTime: 2014-02-18T10:16:49.990 - UID: OMVSDGRPAAABSYSRO01 - LogonID: USER02 - LIDuser: {Acctg, Scty Off} - LIDname: PETER SMITH - LIDupdt: 2014-02-18T10:16:49.990 - LIDpwChg: 2014-02-18T10:15:45.687 - LIDmaskDSN: USER02 - LIDtsoPfx: USER02 - New: {CICS: Yes - GROUP: USERGRP}

SAMPLE RACF VIOLATION AS REPORTED BY AMI DEFENDER FOR Z/OS TO A SIEM

Feb 18 12:50:29 MVSSYSB RACF: EventDesc: RESOURCE ACCESS: Insufficient Auth - UserID: SU018B - Group: RESTRICT - Auth: Normal check - Reas: {AUDIT option} - JobNm: SU018BTR - UID: SU018B - Res: SYS1.PROD.PROCLIBT - Req: READ - Allow: NONE - Vol: SYS001 - Type: DATASET - Prof: SYS1.PROD.PROCLIBT - Owner: DATASET - Name: TONY JOHNSON - SessType: Int Rdr Batch Job - POEclass: JESinput - POE: INTRDR

SAMPLE FTP CLIENT DATA

One of your mainframe users accessing an outside host

Feb 18 12:50:28 MVSSYSB TCP/IP: Subtype: FTP client complete - Subsys: JES2 - Stack: TCPIP - AS: SU018BFT - SubCmd: RETR - FileType: SEQ - RemtDataIP: ::ffff:187.10.8.51 - RemtCtlIP: ::ffff:187.10.8.51 - RemtID: SU018B - LocID: SU018B - DStype: Seq - Start: 2013-07-30T15:41:22.340 - Dur: P00:00:00.010 - Bytes: 15063 - LReply: 250 - Host: mvssysb - FName: PROD.PAYROLL.CHANGES - Security: {Mech: None - CtlProt: None - DataProt: None - Login: Undefined} - RemtUserID: SU018B

SAMPLE FTP SERVER DATA

An outside user successfully copying a file from your mainframe

Feb 18 12:52:40 MVSSYSB TCP/IP: Subtype: FTP server complete - Stack: TCPIP - AS: FTPD1 - Op: Retrieve - FileType: SEQ - RemtDataIP: ::ffff:187.10.8.51 - RemtCtlIP: ::ffff:187.10.8.51 - UserID: SU018B - DStype: Seq - Start: 2014-07-08T14:10:21.460 - Dur: P00:00:00.190 - Bytes: 11176 - LReply: 250 - SessID: FTPD100053 - FName: PROD.CREDIT.LOG - Security: {Mech: None - CtlProt: None - DataProt: None - Login: Password}

SAMPLE FTP SERVER LOGON FAILURE

An unauthorized user attempting to access your mainframe

Feb 18 12:52:38 MVSSYSB TCP/IP: Subtype: FTP server logon fail - Stack: TCPIP - AS: FTPD1 - RemtIP: ::ffff:187.10.8.51 - LogonUserID: IBMUSER - Reas: Password invalid - SessID: FTPD100052 - Security: {Mech: None - CtlProt: None - DataProt: Undefined - Login: Password}

SAMPLE DB2 AUDIT DATA

Feb 18 12:50:28 MVSSYSB Db2: Subsys: DA1L - IFCID: 361 - IFCID_D: Audit administrative authorities - AuthID: SU018B - Conn: BATCH - CorrID: SU018BDC - UserID: SU018B - Trans: SU018BDC - WrkSta: BATCH - OpID: SU018B - Plan: DSNBIND - Loc: NA01DA1L - LUWID: USCSB.NA01DA1L.cbbccb94d2e3.1 - AuthType: SYSADM - AuthIDType: AuthID - ObjType: Package - Priv: Execute - SrcQual: SU018PHN - Src: *

SAMPLE MESSAGE FROM CONSOLE MESSAGE TRAP

(notice): Feb 15 19: 39: 18 mvssyst CZASEND: TSU09177 - XM018R - DEVPROC - DEVPROC - IEF450I JOBABC S1ABEND - ABEND= S806 U0000 REASON= 00000004 874

FOR MORE INFORMATION

AMI Defender for z/OS is available in a complimentary 30-day trial package. To receive a trial of AMI Defender or other BMC trial downloads, please visit **www.correlog.com/download**. For more information on our products, please visit **www.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

511248