BMC AMI Defender

Stream critical mainframe data to your enterprise analytics engines in real-time

PRODUCT DESCRIPTION

BMC AMI Defender is the market’s leading solution for integrating the mainframe into enterprise analytics engines like Splunk and ELK as well as all leading security information and event management (SIEM) solutions like ArcSight, QRadar, or LogRhythm. This integration provides an organization a unified, multi-platform view of their enterprise in a single console.

KEY FEATURES

- **Real-Time Data Stream** – Move from batch intervals to a stream of data presented in real-time to speed detection and response to potential issues. Add your own custom records using our API.
- **Log Filtering** – Receive only the data you need most to minimize resource consumption and storage requirements.
- **Out-of-the-box Formatting** – Data is ready for delivery to leading enterprise analytics engines or SIEMs when installation is complete.
- **Actionable Intelligence** – Logs are enriched with valuable context to help you understand the root causes and potential areas that require further investigation without combing through SMF records.
- **Lightweight** – Impact to the mainframe is kept low with minimal resource consumption leveraging techniques like zIIP offload to safeguard uptime and productivity.
- **Extensive** – Access records across your LPARs, add custom records through an API, and scale across your enterprise with no service degradation.

PRODUCT DETAILS

- **Continuous Security Monitoring** – detect anomalous and malicious activity occurring on the mainframe. Automatically identify and alert you when access to core OS files, sensitive datasets, or password databases occur. Potentially malicious activities like anomalous read/write activity can also be uncovered to halt ransomware or data exfiltration techniques like FTP, IND$File, or NFS.
- **Enterprise-wide Visibility and Transaction Tracing** – the mainframe does not operate in a silo which necessitates a single integration point across all systems for complete 360-degree operational visibility.

- **User Entity Behavior Analytics** – provide detailed analysis and correlation of user behavior. Enriched records provide the user ID, name, and point of entry to every log.

- **Privileged User Monitoring** – monitors and supervises the most critical users on the system. The user’s credentials will be added to each log and users that have modified their privileges will be automatically detected and flagged to surface potential privilege escalation-based attacks.

- **Performance + Operations Analytics** – monitor and diagnose IT problems across the full spectrum of IBM® z/OS®, IBM® Db2®, and IBM® IMS®.

- **Achieve Compliance** – immediately meet multiple compliance requirements set forth by PCI DSS, HIPAA, IRS Pub. 1075, GLBA, SOX, FISMA, NERC, and many others.

- **Database Activity Monitoring** – deep Db2 and IMS support extend ability to conduct each of the above use cases at the database level with real-time monitoring of privileged database administrators and auditing for all Db2 and IMS access, write, and read activity. Our unique approach gives you complete access to all database activity in your enterprise analytics engine with minimal system overhead.

### BMC SOLUTION

BMC AMI Defender is a lightweight agent that installs quickly, uses minimal resources, and does not require extensive training, ongoing maintenance, or administration. The agent resides on an LPAR that monitors all activity happening on the mainframe and, in real-time, filters the data for relevant information and formats it into either RFC 3164 Syslog, JSON, LEEF, CEF, or even CIM (Splunk) before sending it to the enterprise SIEM or analytics engine. The messages arrive ready-formatted, so no further processing is required, and analysts can gain immediate insights through your existing or preferred tool.

### DATA SOURCES

- RACF/ACF2/Top Secret
- Networking data (FTP, TCP/IP)
- Db2 / IMS
- Resource Measurement Facility
- IBM® CICS® transactions
- JES / JES JOBLOG
- USS
- IBM® MQ®
- IBM® WebSphere®
- Log4J
- CL/SuperSession
- z/OS console messages
- TSO
- IND$FILE
- BMC Compuware Abend Aid & Application Audit
- Action Software International EventAction
- Micro Focus ChangeMan
- Hardware Management Console
- And many more

### ENRICHMENT

- User ID of the user associated with the job
- User’s full name
- User’s privileges
- Job ID
- Type of work: batch job, TSO session, or started task
- Name of the program from the JCL EXEC statement
- Job “port of entry” – whether it came from the internal reader, RJE, a system command, and so forth
- Tags APF authorized dataset
- Identifies any use of a dynamic APF command
- Tags key operating system files like PROCLIB/PARMLIB
- Tags dataset encryption key files
- Tags ESM databases
- And many more

### FOR MORE INFORMATION

If you’re interested in seeing how your organization can benefit from greater insights and visibility, and how to extend the value of your existing analytics and security tools, a **complimentary 30-day trial** is available. For more information on our mainframe security products, please visit [bmc.com/ami-security](http://bmc.com/ami-security).