Datasheet

BMC AMI Security

Continuously protect your mainframe with automatic detection, response and actionable insights

PRODUCT DESCRIPTION

BMC AMI Security automatically protects, detects, and responds to threats on your mainframe. Acting as a virtual security expert, it uses out-of-the-box policies to harden the mainframe environment against vulnerabilities, insider threats, and data theft. Actionable insights help incident responders investigate and close the window of opportunities for hackers.

BUSINESS CHALLENGE

As an enterprise system with sensitive data and a host of internal and remote connections, the mainframe is a rich target for attackers. However, mainframe teams and enterprise security leaders often lack effective visibility into vulnerabilities on mainframe systems. This leaves the environment vulnerable to zero-day threats, configuration weaknesses, and attacks like ransomware—putting sensitive data at constant risk. In fact, real-world penetration testing shows the average mainframe has over 100 severe vulnerabilities and can be compromised in as little as six minutes. A shortage of mainframe skills and resources compounds the challenge. To protect the business, organizations need real-time visibility into mainframe vulnerabilities and threats, as well as accurate, automated tools for rapid detection and response.

BMC SOLUTION

BMC AMI Security lets you secure your mainframe like any other system so you can detect and respond to threats, aid compliance, and reduce risk without the need for specialized mainframe expertise. Details on threats and vulnerabilities are shared to your SIEM in real-time. Responses to threats can be performed automatically or manually and use behavioral analytics to halt both suspicious and known malicious actions. Indicators of compromise (IOCs) are translated into common security terms for a fast, effective response by security analysts.

KEY FEATURES

- Continuous, automated protection, detection, and response to mainframe security events
- Enterprise SIEM integration for real-time threat visibility
- Actionable intelligence in common security terms for fast, effective incident response
- Out-of-the-box policies and the industry's largest library of Indicators of Compromise (IOCs)
- Web-based console and preconfigured dashboards for simple, efficient administration

KEY BENEFITS

- Improve uptime by automatically preventing threats, halting attacks before a compromise and reducing MTTR
- Break silos between SOC and operations teams with shared visibility into mainframe security events
- Overcome the mainframe skills gap with automation, efficiency, and built-in intelligence
- Reduce risk and strengthen your security posture with configurations and recommendations driven by mainframe hacking experts
- Address compliance with alerts, audits, reports, and comprehensive mainframe visibility

PRODUCT DETAILS

Automated Protection, Detection, and Response

Stop threats before they can disrupt your mainframe environment or put sensitive data at risk.

- Continuous mainframe and database monitoring detect suspicious activity in real-time
- Suspicious and known malicious actions are automatically halted or you can be alerted in order to take action manually
- Real-time behavioral analytics trigger alerts for known Indicators of Compromise (IOCs)
- Risks and configuration vulnerabilities are uncovered and surfaced continuously to help harden the mainframe against threats
- Software vulnerability scans identify zero-day exploits

Integration with Leading SIEM Systems

Achieve real-time, shared visibility for SOC and operations teams into current vulnerabilities, threats, and activity.

- Mainframe security events are delivered to your security team's SIEM of choice to close the window of opportunity for attackers
- Tickets are created automatically for instances requiring attention
- Attacker actions are logged and tracked on a timeline including the vulnerabilities and methods used to guide your response

Actionable Intelligence for Incident Response

Accelerate response and shorten MTTR with clear, accurate, and actionable insights.

- IOCs on the mainframe are translated into common security terms and alerts are delivered in real-time
- Data is automatically correlated across multiple systems to see actions in context; events considered to be normal are learned over time to reduce alert noise
- Real-world penetration tests continuously refine and inform IOCs for the most accurate alerts possible

Simplified, More Efficient Administration

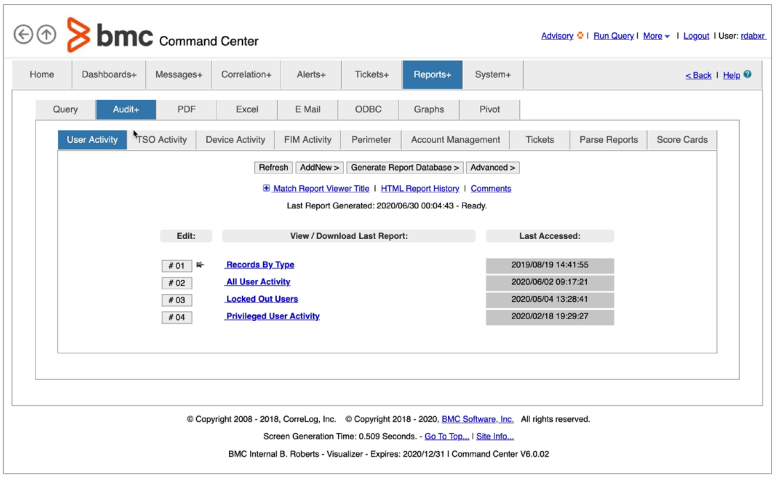
Help your mainframe team get more done, with greater simplicity.

- An intuitive web-based console for RACF administration removes the need for mainframe skills and boosts helpdesk productivity
- Automated password administration eliminates the burden of frequent password reset requests for better security and service desk efficiency
- Pre-configured, dashboard-style views of mainframe activity help admins visualize cross-platform security events system-wide

Alerts, Audits, and Real-Time Visibility

Facilitate compliance with key mandates including HIPPAA, PCI DSS, and GDPR.

- Customizable alerts let you specify actions or threat events unique to your environment
- An audit trail of events across z/OS, Db2, and IMS production systems simplifies regulatory compliance
- Reports on system policies, configurations, and current health provide full visibility across your mainframe environment



FOR MORE INFORMATION

To learn more about BMC AMI Security, please visit **bmc.com/ami-security**

About BMC

From core to cloud to edge, BMC delivers the software and services that enable over 10,000 global customers, including 84% of the Forbes Global 100, to thrive in their ongoing evolution to an Autonomous Digital Enterprise.

BMC—Run and Reinvent **www.bmc.com**

523314