BMC Compuware Application Audit

Strengthen mainframe cybersecurity and compliance with rich user behavior intelligence

PRODUCT DESCRIPTION

BMC Compuware Application Audit enables enterprises to capture all relevant data about user access and behavior on the mainframe to mitigate cybersecurity risks and fulfill compliance mandates.

BUSINESS CHALLENGE

While the mainframe is the enterprise’s most intrinsically secure platform, businesses must still proactively protect mainframe systems and data against cybersecurity threats. Data breaches are often not discovered until days or months after the fact, if at all, resulting in massive costs to the business, forced public disclosures, and irreparable brand damage. Enterprises must have the ability to capture and analyze mainframe application session user activity in real time to reduce the risk of potential breaches.

Most enterprise security teams rely on disparate logs and SMF data from security products to monitor their environments, track activities, and send alerts when attacks and suspicious events take place. However, these tools typically only capture data about who is logging in and out and when, or when unauthorized attempts are made to access systems, applications, and data. Overall, the data provides little visibility into end-user activities, including whether a user accessed sensitive data and what they did with it, leaving security teams with blind spots.

BMC SOLUTION

BMC Compuware Application Audit enables security and compliance teams to easily capture start-to-finish mainframe user behavior in real time, including all successful logins, session keyboard commands and menu selections, and specific data viewed, without making any changes to mainframe applications.

KEY FEATURES

- Gain deep insight into user behavior, including data viewed, by whom, and which applications were used to access it
- Detect, investigate, and respond to inappropriate activity by internal users with access and/or hacked or illegally purchased user accounts
- Deter insider threats by capturing and analyzing start-to-finish user session activity
- Integrate user behavior intelligence with popular SIEM engines to analyze the overall application environment
- Support criminal/legal investigations with complete and credible forensics
- Deliver granular intelligence and reporting capabilities needed to comply with regulations such as HIPAA, GDPR, the Australian NDB scheme, as well as company security policies
- Separate the system administrator’s duties from mainframe-inexperienced auditor’s responsibilities with a web UI, so that no single person is in a position to engage in malicious activities without detection

KEY BENEFITS

- Reduce risk and liability associated with production security and compliance
- Lower cost of regulatory compliance
- Provide vital forensic evidence of suspicious activities
- Improve rapid response for auditing infractions

BMC Compuware Application Audit lets you easily create recording requests. Application Audit’s intuitive web interfaces make it easy for security personnel with no mainframe experience to set session recording parameters, enable the data to be delivered to SIEM systems, and review recording activities.
**PRODUCT DETAILS**

**SIEM integrations for comprehensive intelligence**

Enterprises can automatically deliver Application Audit data to SIEM engines such as Splunk, Elasticsearch, IBM QRadar®, and HPE ArcSight ESM directly or in combination with BMC AMI Defender for z/OS® or Precisely Ironstream®.

Analytics-rich dashboards provide organizations with a larger picture of their overall application environment. With this coverage, personnel can spend more time on scrutinizing legitimate threats and determine the true end-to-end user activity for applications.

**Intuitive web user interface**

Application Audit’s intuitive web UI empowers security and compliance staff to set session recording parameters, review recording activities, enable the data to be delivered to SIEM systems, and perform other administrative tasks.

The UI also enables separation of the auditor role, who has no mainframe expertise, from the system administrator’s duties, so that no single person is in a position to engage in malicious activities without detection.

**Out-of-the-box integrations and dashboards**

Application Audit provides an out-of-the-box Splunk-based dashboard to view a multitude of statistics around user behavior including users by LPAR, users by session duration, users with invalid transactions, transactions not recognized by LPAR, and more.

Application Audit user behavior data is also directly integrated into BMC AMI Security, enabling better user and entity behavior analytics (UEBA) for faster detection of malicious activities.

**KEY BENEFITS (CONTINUED)**

- Achieve near real-time insights that fuel faster mitigation, strengthening security
- Identify and reduce cybersecurity threats with SIEM integrations that provide vital mainframe application-level insight
- Improve data breach detection and contain and reduce data breach impacts
- Eliminate dependency on specialized mainframe knowledge

---

**FOR MORE INFORMATION**

To learn more about BMC Compuware Application Audit, visit [bmc.com](http://bmc.com).

---

**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**

---

**BMC Compuware Application Audit** provides an out-of-the-box Splunk-based dashboard to view a multitude of statistics around user behavior. User behavior data is directly integrated into BMC AMI Security enabling better entity behavior analytics for faster detection and malicious activities.