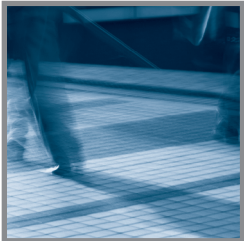# BMC Software
Meets Sarbanes-Oxley Compliance with IPLocks

In today's environment of increasing government regulations, battling the compliance process can be arduous and time consuming. Auditors have high expectations for reporting and IT controls across the enterprise. BMC Software was no exception. Regardless of how organized and protected the company was in the past, yesterday's security measures no longer guarantee successful regulatory compliance.

BMC Software is a $1.46 billion, Fortune 1000 global leader in enterprise management solutions. BMC places a high value on effectively managing their complex IT environment, especially since it provides these services to their customers.

CHALLENGE: GREATER CONTROLS FOR SARBANES-OXLEY COMPLIANCE

BMC needed to establish greater controls and business processes for information risk management in order to fulfill Sarbanes-Oxley (SOX) requirements. BMC relied on time-consuming manual processes for tracking database changes and finding security policy violations. Unless they knew exactly when and where to look, many important database changes and policy breaches could easily go undetected. While BMC never had a major security breach, the lack of visibility and monitoring could one day be an issue.

SOLUTION: IPLOCKS DATABASE SECURITY AND COMPLIANCE

BMC's main priorities for meeting SOX compliance for information risk management were increasing visibility and improving controls. Since BMC needed to know when changes were made to critical databases and when access policies were violated, they turned to IPLocks Database Security and Compliance Solution.

The first step of the audit process was to define BMC's most critical business databases. These included a large Oracle financials system, a Siebel Systems sales and customer database, and other databases that managed expense reporting and professional services data. SOX warned that these systems were at the greatest level of risk

for malicious acts since they contained highly sensitive data. If a security breach ever occurred, there would be a significant and adverse impact on BMC's business. While other databases existed throughout the company, BMC initially ran the IPLocks Solution against these critical databases to meet the SOX requirements.

BMC KEEPS VIGILANT WATCH, MONITORING FOR INFORMATION RISK

The Metadata Monitor function of the IPLocks Solution allowed BMC to automatically scan critical databases for changes in key data tables and generate reports. Since the larger databases had tens of thousands of changes, the results were filtered according to the level of importance or risk. More serious updates, such as a developer changing a production package or altering certain tables, were flagged while routine processes were filtered out. Because IPLocks is an agentless application, the remote scans were conducted using inconsequential performance and resource overhead. With Oracle's full audit capabilities running and IPLocks solution deployed, the database server performance overhead was less than three (3) percent.

BMC also relied on the IPLocks Privilege Monitor functionality to keep vigilant watch on the SOX critical databases. The application monitors data access on a regular basis to ensure there are no security breaches. This capability was critical in helping BMC ensure employees follow security policies. The regular reports and alerts indicated any unusual activity, such as a suspiciously high

number of users connecting with the same user name and password.

Over 900 BMC employees have regular access to the sales and customer database alone. Using the standard monitoring and reporting capabilities in the IPLocks Solution, BMC now keeps a close watch on changes such as altering access privileges and granting new employee access. The ongoing reports indicate trends to establish a baseline for normal behavior and to discern unusual activities that require action.

CREATING AND SIMPLIFYING THE SOX AUDIT TRAIL

With the new risk management policies in place, BMC runs reports for both Metadata Monitor and Privilege Monitor. These reports are distributed via email to managers responsible for the business critical databases. These managers review the activity and approve each report, denoting whether or not actions should be taken. This process ensures that management and the database application owner are informed and actively involved in improving the risk management levels. The IPLocks Solution has made it simple for BMC to prioritize, group, and approve issues found in reports. Since both reports and management signoffs are logged, a valuable information trail for the SOX auditors is created.

To date, BMC's focus has been on the SOX compliance. Moving forward the company plans to ensure even greater information risk management. Future plans include implementing the IPLocks Vulnerability Assessment Solution to provide a security level score for each critical database. This

"IPLocks enables us to proactively manage database risks and automate data collection procedures required by auditors for Sarbanes-Oxley compliance."

Randy Scheers
Manager, Database Administrators

assessment will give BMC valuable information to prioritize security improvements. With the IPLocks Vulnerability Assessment Solution, BMC can quickly and easily distinguish between databases with high levels of security and those that need to be altered to prevent future breaches. This important next step will improve BMC's information risk management strategy while demonstrating progress to auditors.

For companies like BMC who undergo annual audits and changing regulatory requirements, achieving SOX compliance continues to be a top priority. By creating an audit trail, the IPLocks Database Security and Compliance Solution is helping BMC to win the SOX compliance battle. While SOX initially seems overwhelming and time consuming, adding IT controls and business processes eventually make IT more efficient and accountable. By implementing the IPLocks Solution, BMC now has greater visibility into their most strategic data sources and a better understanding of the activities and changes happening within their IT environment.

Rev 2   03/06