SOLUTION BRIEF

Monitor IBM i (AS/400) Database Activity and Security Alerts

Integrate auditing and compliance capabilities from IBM i with data from other platforms

Enterprises often run business-critical applications on IBM i (AS/400) systems, as well as other hardware platforms. To maximize database visibility and protection across these platforms and integrate security alerts from all possible sources of attacks, enterprises need a way to integrate relevant data originating on the IBM i into the McAfee® architecture. Raz-Lee iSecurity for McAfee® Database Activity Monitoring and McAfee Enterprise Security Manager provides precisely this capability, which helps global, multiplatform customers deter database attacks, monitor external threats, and analyze and respond to cross-platform threats quickly and effectively.

McAfee Compatible Solution

- iSecurity 12.7 for McAfee Database Activity Monitoring 4.4.8 and McAfee Enterprise Security Manager

McAfee and Raz-Lee Joint Solution

Companies of all sizes across all industry sectors are finding that they need advanced risk management capabilities in these areas:

Auditability

- Built-in, simple-to-modify Microsoft Windows-like reports for external and internal auditors that can be scheduled to execute when appropriate and that can be emailed to relevant managers and technical staff for review
- Ability to audit system infrastructure and application-related events, so real-time alerts of these events can be sent to operations personnel as syslog messages

Compliance

- Adherence to corporate and industry standards and regulations, such as Payment Card Industry Data Security Standard (PCI-DSS), Sarbanes–Oxley (SOX), Health Insurance Portability and Accountability Act (HIPPA), and others
- Ready-to-run, easy-to-adapt compliance checklists for periodic assessments

Security

- Minimization of risk and liability by stopping attacks before they cause any damage

The joint McAfee-Raz-Lee solution for databases addresses these concerns via IBM i system and database sensor data, including SQL and traditional IBM i input/output (I/O) data. This information is passed to the McAfee® ePolicy Orchestrator® (McAfee ePO™) security management console via intermediate stages of filtering and transmission. Seamless integration ensures successful transmission of all relevant data and provides McAfee Database Activity Monitoring with a complete log of all the information it requires for cross-platform database activity monitoring and analysis. McAfee ePO console customers who depend on the security management system to provide end-to-end visibility into database security with both summary and detailed event information are assured that their analysis, reports, and decisions are based on true IBM i I/O log data.

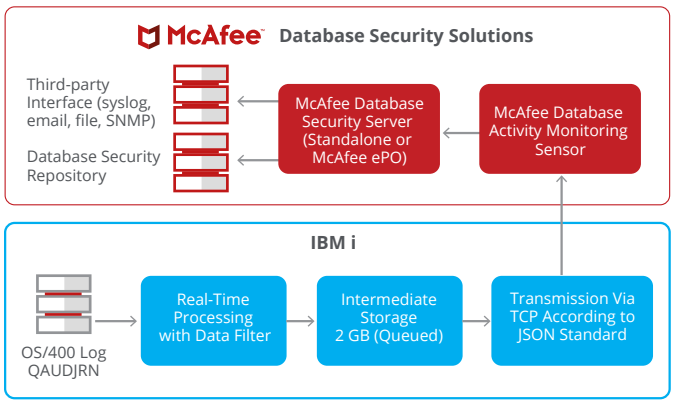

Figure 1. Seamless integration of Raz-Lee iSecurity and McAfee ePO software provides McAfee database security solutions with visibility to IBM i log and threat data.

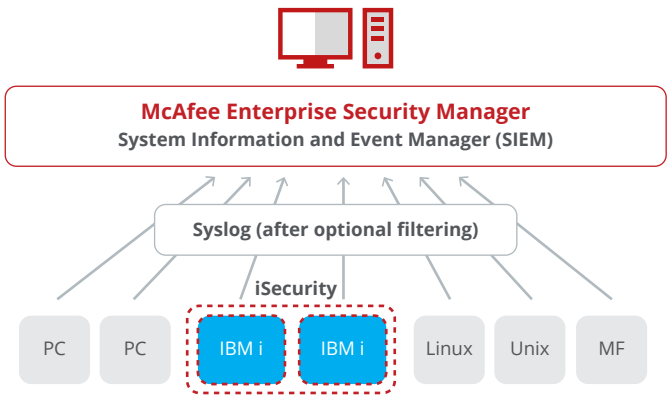

Figure 2. The joint McAfee and Raz-Lee SIEM solution facilitates swift detection of cross-platform breaches.

The joint McAfee-Raz-Lee security information and event management (SIEM) solution provides McAfee Enterprise Security Manager with security-related information from the IBM i, which, when integrated with data from other platforms, maximizes McAfee Enterprise Security Manager's forensic capabilities to ensure that cross-platform security breaches are detected quickly and accurately.

About Raz-Lee Security

Raz-Lee Security is the leading security solution provider for IBM i (AS/400) computers. Drawing on more than 33 years of experience in the IBM i performance and optimization market, Raz-Lee designs, develops, and XSsoftware solutions. iSecurity is field-proven at thousands of sites worldwide in more than 40 countries—ranging from sites with more than 200 systems to small and medium-size businesses and single-LPAR P05 installations.

About McAfee Enterprise Security Manager

McAfee Enterprise Security Manager—the foundation of the McAfee SIEM solution family—delivers the performance, actionable intelligence, and real-time situational awareness at the speed and scale required for security organizations to identify, understand, and respond to stealthy threats, while the embedded compliance framework simplifies compliance.

About McAfee Database Activity Monitoring

McAfee Database Activity Monitoring—part of the McAfee solution portfolio—finds databases on your network, protects them with preconfigured defenses, and helps build a custom security policy for enterprise environments. Organizations gain visibility into all database activity, including local privileged access and sophisticated attacks from within the database. McAfee Database Activity Monitoring helps protect valuable, sensitive data from external threats and malicious insiders. In addition to providing a reliable audit trail and making it easy to demonstrate compliance, McAfee Database Activity Monitoring also prevents intrusion by terminating sessions that violate security policy.

McAfee
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

62246brf_razlee-esm-dam_0216
FEBRUARY 2016