

SIEM and Log Management for Converging Network and Security Environments

Two-way Exchange of Security Events between McAfee ePolicy Orchestrator and QRadar

Q1 Labs, a leader in the security information and event management (SIEM) market, has integrated their flagship product, QRadar, with network and endpoint systems technologies across the McAfee portfolio. QRadar intelligently distills large amounts of information from a wide range of sources to augment incident response and compliance validation in McAfee ePolicy Orchestrator® (ePO™) software, McAfee's centralized security and compliance management platform.

Business Problem

Companies are continually required to address a wide range of security issues that include threat protection, compliance management, audit response and fraud detection while being mindful of operational goals and cost containment. Products used to address these issues are compartmentalized and often narrowly focused, resulting in operational inefficiencies and difficulties in achieving compliance and audit goals.

An infrastructure that can bring together data from a wide array of sources (endpoint and network) while providing intelligent analysis and alerting to the right personnel at the right time is critical to achieving overall security goals in a cost effective manner.

McAfee + Q1 Labs Solution and Benefits

Solution Overview

Q1 Labs has achieved a unique position in the SIEM market by redefining how organizations deliver centralized network security management. McAfee has partnered with Q1 Labs to offer mutual customers a unified endpoint and network security solution that integrates the analysis and correlation of large amounts of disparate data into a single solution. Q1 Labs' QRadar system collects data from a wide range of security device types and manufacturers as well as flow data. Specific to McAfee, supported products include:

- McAfee ePolicy Orchestrator
- McAfee Network Security Platform (formerly IntruShield)
- McAfee Vulnerability Manager (formerly, Foundstone Enterprise)
- McAfee Secure Firewall (formerly, Secure Computing's Sidewinder)
- McAfee Secure Web (formerly, Secure Computing's WebWasher)

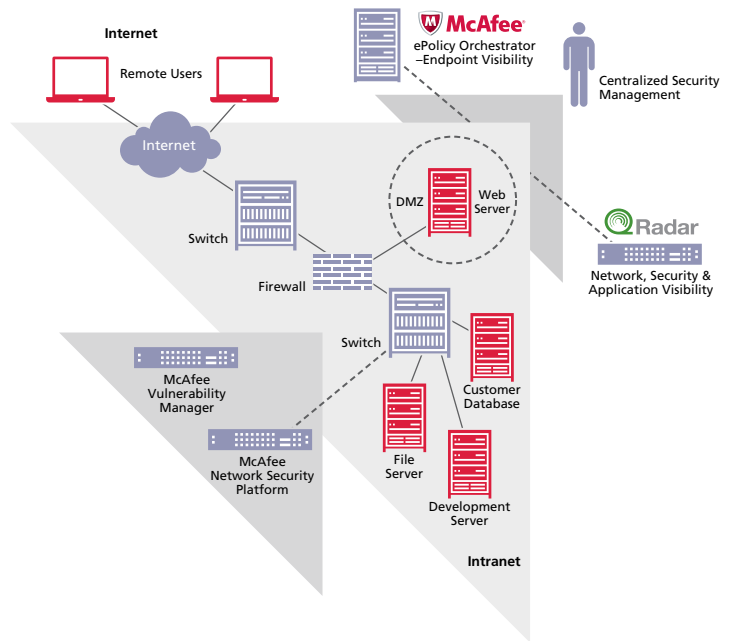


The QRadar system normalizes, aggregates, and correlates security event and network flow data, delivering to the user a prioritized list of issues or offenses that need investigation. The analysis

Solution Brief SIEM and Log Management for Converging Network and Security Environments

of security event and network flow data together adds context thereby minimizing false positives and reduces the time to resolution by ensuring the McAfee ePO software user has all supporting data a simple mouse click away, regardless of which vendor's product triggered the alert.

The integration of QRadar and McAfee ePO software is bidirectional. Events in the ePO database are sent to QRadar for analysis. Additionally, offenses (alerts) that are generated by QRadar are sent to the ePO database to alert the ePO software operator who can then take the appropriate remediation action.



Benefits

Together the McAfee ePO software and QRadar solution provide:

- **Enhanced Threat Protection:** The joint solution integrates endpoint security, network security, and incident reporting.
- **Improved Compliance Management:** QRadar's ability to consolidate data from McAfee's product suite with other network and security products provides customers with a single point for investigation and reporting in support of their audit and compliance requirements (such as PCI and SOX).
- **Log Management:** Logs from a wide range of devices are consolidated for forensics and storage.
- **Better Operational Efficiencies:** By providing the right data, to the right user, at the right time, the joint solution uses a better workflow to improve visibility and lower time to problem resolution.

McAfee Compatible solution: QRadar 6.1.3 and McAfee ePO 4.0.

About McAfee Security Innovation Alliance

The McAfee Security Innovation Alliance is the foundation of a technology ecosystem designed to assemble the world's leading security innovations. Working together, McAfee and its partners deliver solutions more comprehensive than those available from any single vendor. You'll find the McAfee Compatible logo on products that have passed McAfee's integration testing. For more information, visit www.mcafee.com/sia.

About McAfee, Inc.

McAfee is the world's largest dedicated security technology company. McAfee relentlessly tackles the world's toughest security challenges. With nearly 350 patents, our award-winning research team and engineers develop solutions that make businesses more powerful to protect their systems, networks, and data, while also helping them optimize complex risk and compliance issues. At home, we help consumers secure every aspect of their digital life—PC, mobile phone, and internet—with solutions that auto-update and are easy to install and use.

