

QRadar VFlow

Delivering Cost Effective Visibility in Virtual Environments

Application Layer visibility and content awareness for all corners of your virtual infrastructure.

Define, Implement, and Protect Virtual Servers

The use of virtualized servers is now becoming common in IT infrastructures across businesses of all sizes and industry. Since its conception, virtualization technologies have successfully moved from the lab, to test environments, to full production. There are many benefits of virtualization including improved use of networked systems, cost reduction, and simplified management. Virtualization however creates additional challenges when implementing strong security controls, such as being able to monitor traffic traversing virtual environments, that cannot be collected from traditional monitoring technologies.

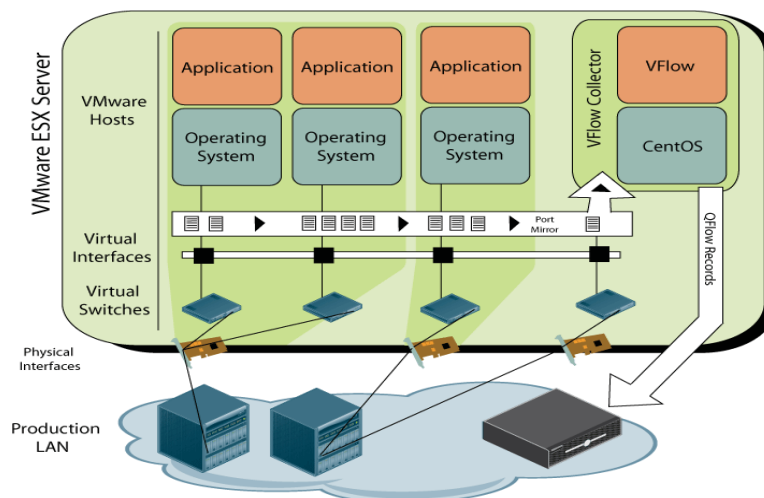
Visibility is Key to Securing Any Network, Including Virtual Environments

Common wisdom, as with any new technology, is that organizations should continue following existing IT security best practices, including log management and security information and event management (SIEM), and leverage new technologies that are focused on solving specific security challenges introduced by virtualization. For virtualized companies, QRadar® VFlow provides advanced security intelligence in virtual environments by providing application layer visibility of all virtual network traffic. By adding QRadar VFlow to the QRadar Security Intelligence Platform it provides organizations with an easy to use, cost effective, security intelligence solution. The result—greatly improved security of the virtual network.



QRadar® VFlow provides advanced Security Intelligence in virtual environments by providing application layer visibility of all virtual network traffic.

- Improved Layer 7 visibility
- Cost effective
- Efficient virtual network monitoring



QRadar VFlow

Delivering Cost Effective Visibility in Virtual Environments

Features and Benefits Specific to QRadar VFlow:

Improved visibility

QRadar VFlow provides layer 7 visibility for VMware ESX and ESXi virtual environments; enables the profiling of over 900 applications out-of-the-box

Cost effective

QRadar VFlow runs as virtual host software on the virtual server, not requiring additional hardware; Can analyze port mirrored traffic for a physical network switch which helps bridge the gap between the physical and virtual realm

Efficient virtual network monitoring

QRadar VFlow provides network and application visibility in both existing and emerging virtual networks

QRadar VFlow is one of many modules that can be leveraged by the QRadar Security Intelligence Platform.

Benefits of adding QRadar VFlow to QRadar Security Intelligence Platform include:

Centralized command and control console

Integrated log management, security information and event management (SIEM), Risk Management and network and application visibility in a single console improves IT operational efficiency.

Network, security, application, & identity awareness

Converged monitoring of network events, security events, network and application flow data, virtual network activity, vulnerability data, and identity information greatly improves ability to detect threats.

Advanced threat and security incident detection

By incorporating new analytics techniques, like behavior analysis, and broader intelligence, QRadar helps reduce false positives and detect threats that other security solutions miss.

Compliance-driven reporting capabilities

A comprehensive library of security reports enables the delivery of IT best practices which support compliance initiatives.

Scalable distributed log collection and archival

QRadar's distributed appliance architecture scales to provide event and flow log management in any enterprise network.

Cost effective security management solution

Built upon three pillars of intelligence, integration and automation, QRadar provides a solution that is cost effective to acquire, deploy, and maintain.

Technical Specifications

- Requires VMware ESX 3/5 and ESXi 3.5
- Requires at least 512 MB RAM
- Provides collection of up to 10,000 Flows per Minute (FPM)
- Provides collection of up to 4 virtual interfaces

Q1 Labs
890 Winter Street, Suite 230
Waltham, MA 02451 USA
1.781.250.5800, info@Q1Labs.com

Copyright 2011 Q1 Labs, Inc.
All rights reserved. Q1 Labs, the Q1 Labs logo, Total Security Intelligence, and QRadar are trademarks or registered trademarks of Q1 Labs, Inc. All other company or product names mentioned may be trademarks, registered trademarks, or service marks of their respective holders. The specifications and information contained herein are subject to change without notice.

DSQRFV0711