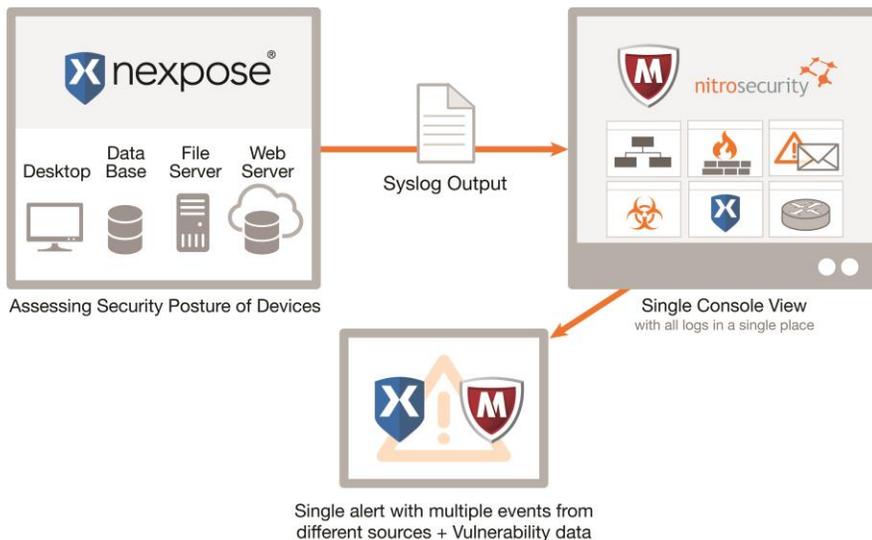# RAPID7

Total Security Visibility with Rapid7's Vulnerability Intelligence data within McAfee Enterprise Security Manager

Solution Overview

For today's IT and Security Operations teams the need for a centralized logging and correlation tool has become a major cornerstone for most organizations. By leveraging Rapid7's rich vulnerability and exploit data, an organization can leverage this information in conjunction with other log data sources to provide greater context and insight into the events happening within environment. McAfee ESM provides real-time actionable intelligence, meanwhile delivering an efficient and effective incident management workflow. Furthermore, vulnerability and asset data within McAfee ESM streamlines the process of conducting post incident forensic analysis.

How it works

A Nexpose scan is conducted to assess the risk posture of the systems within an organization. The vulnerability data is then taken and used to calculate the RealRisk™ score associated with each system detected. Nexpose forwards scan data via a syslog feed to McAfee ESM. Once the data is in McAfee ESM it can be used to add context which support prioritization of remediation and mitigation activities.

Assessing Security Posture of Devices

Syslog Output

Single Console View
with all logs in a single place

Single alert with multiple events from
different sources + Vulnerability data

Overview of Integration Process

> Step 1: Nexpose performs security assessment

> Step 2: Configure Nexpose to forward scan data via syslog

> Step 3: McAfee ESM needs to be configured to accept data source

> Step 4: Vulnerabilities get stored for retrieval

Integration Benefits

> **Security Context Awareness** into the vulnerability state of assets

> **Single Pane View** into your security events, reporting, forensics, and incident investigation.

> **In Depth Investigations** with additional security information about each asset (ports, services, applications, etc.)

> **Automated Vulnerability** data import via syslog when a vulnerability scan completes

Solution Components

What you need:
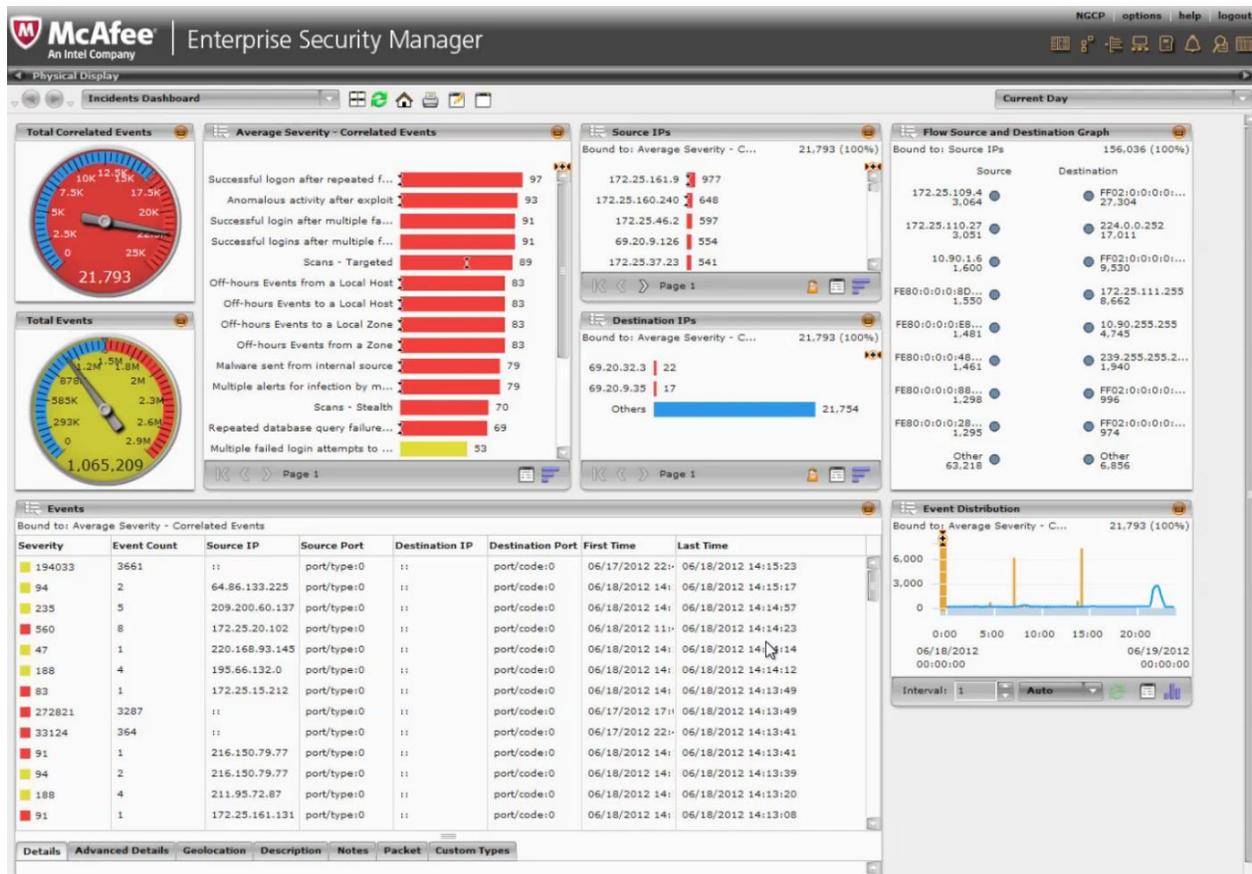
> **Rapid7 Nexpose 5.x**

> **McAfee ESM 9.x+**

Figure1: Screenshot of McAfee Enterprise Security Dashboard

About McAfee

McAfee is the world's largest dedicated security technology company. Delivering proactive and proven solutions and services that help secure systems and networks around the world, McAfee protects consumers and business of all sizes from the latest malware and emerging online threats. Their solutions are designed to work together, integrating antimalware, antispyware, and antivirus software with security management features that deliver unsurpassed real-time visibility and analytics, reduce risk, ensure compliance, improve internet security, and help businesses achieve operational efficiencies.

About Rapid7

Rapid7's security solutions deliver visibility and insight that help you make informed decisions, create credible action plans, and monitor progress. They simplify risk management by uniquely combining contextual threat analysis with fast, comprehensive data collection across your users, assets, services and networks, whether on premise, mobile or cloud-based. Rapid7's simple and innovative solutions are used by more than 2,500 enterprises and government agencies in more than 65 countries, while the Company's free products are downloaded more than one million times per year and enhanced by more than 200,000 members of its open source security community. Rapid7 has been recognized as one of the fastest growing security companies by *Inc. Magazine* and as a "Top Place to Work" by the Boston Globe. Its products are top rated by Gartner® and *SC Magazine*. For more information about Rapid7, please visit http://www.rapid7.com.

Contact us today to learn more

1-866-772-7437

1-866-7-RAPID7