



Sourcefire® and Rapid7

Sourcefire IPS™ and its Awareness Technologies Integrate with Rapid7 for Enhanced Impact Analysis

Sourcefire and Rapid7 Integration Benefits

- Gain additional contextual network detail
- Realize more effective impact analysis
- Expand impact analysis across the network
- Extend your security investment
- Improve network security

Information is critical when your network is under attack. You need to know the composition of the hosts on your networks and the applications that these hosts are running. Contextual network data helps your security analysts prioritize intrusion alerts and assess their malicious intent to more effectively protect your organization against threats. Sourcefire and Rapid7 have partnered to provide you with the powerful contextual network data you need for more effective impact analysis.

Through this collaboration, Rapid7 seamlessly integrates vulnerability data into the Sourcefire IPS. By using the two solutions in combination organizations achieve more effective threat impact analysis covering a wider range of vulnerabilities across more applications, extending current technology investments to increase security.

A CLOSER LOOK AT RAPID7 VULNERABILITY MANAGEMENT AND PENETRATION TESTING SOLUTIONS

Rapid7 solutions include the award-winning vulnerability management solution, NeXpose Enterprise®, and Metasploit Express® for penetration testing. Through an integrated, intelligent, active scan engine, Rapid7 NeXpose identifies vulnerabilities across networks, operating systems, databases, Web applications and a wide-range of system platforms and prioritizes vulnerabilities using exploit risk scoring and asset criticality ratings. Metasploit Express emulates real-world attacks on the network in order to test for the ability to penetrate the vulnerabilities and launch an attack, greatly decreasing the time to test and increasing the efficiency in real threat detection. By understanding how hackers operate, Rapid7 NeXpose and Metasploit Express reduce risk exposure and lower operational costs..

COMBINING ACTIVE AND PASSIVE VULNERABILITY ANALYSIS: A POWERFUL APPROACH

Active and passive vulnerability analysis each has its advantages. An active approach that combines active scanning and penetration testing provides more accurate vulnerability data because it locates vulnerabilities and then mimics attacks to verify vulnerabilities. Passive discovery offers up to the second, 24-hour coverage of your network between active scans, and for Sourcefire, this includes a real-time inventory of operating systems, services, applications, and potential vulnerabilities.

By combining Rapid7 active vulnerability scan data and penetration testing with Sourcefire passive awareness technology, your organization enjoys the best of both worlds. Customers can import Rapid7 scan and penetration testing data into the Sourcefire host database to validate its findings and augmenting host profiles with those vulnerabilities that can only be determined through active scanning. Correlating attack information against the combined vulnerability set results in higher accuracy for Sourcefire's unique Impact Flag scoring, which prioritizes security events. Through this combination of Sourcefire's real-time network discovery information with Rapid7's vulnerability scan and testing data, an organization achieves more effective impact analysis covering a wider range of vulnerabilities across more applications.

BENEFITS OF INTEGRATION

The Sourcefire and Rapid7 integration provides significant benefits, particularly in the following scenarios:

- Additional contextual network detail and more effective impact analysis: Sourcefire awareness technologies detect many applications, but there are some applications that Rapid7 can detect that Sourcefire does not, and vice versa. Adding Rapid7 vulnerabilities to the Sourcefire solution means that impact analysis will be more effective and cover a wider range of vulnerabilities across more applications.
- For example, if an intrusion event references a vulnerability in an application that Sourcefire does not detect, Sourcefire will set the Impact Flag to “Potentially Vulnerable” or “Not Vulnerable.” However, if this vulnerability has been added to the Sourcefire vulnerability database, then the intrusion event will have an Impact Flag of “Vulnerable” because the Sourcefire solution is now aware of the host’s vulnerability.
- Impact analysis expanded to segments of your network not yet monitored by Sourcefire awareness technologies: For example, a large, distributed organization may use Rapid7 to scan hosts in multiple remote sites, but it may not yet have deployed Sourcefire awareness technologies to these sites for cost, time, or management reasons. This organization could import the Rapid7 vulnerability data for these remote hosts into the Sourcefire solution, and impact analysis would be able to correlate against the vulnerabilities found for these hosts.

TAKE THE NEXT STEP TO PROTECT YOUR NETWORK

Learn more about how you can benefit from the combination of leading technology from Sourcefire and Rapid7. Visit us at www.sourcefire.com or contact Sourcefire or a Sourcefire Global Security Alliance channel partner today.