SOURCEfire®

QUALYS® ON DEMAND SECURITY

Sourcefire 3D® System and QualysGuard® Vulnerability Management Integration

Providing Additional Contextual Network Detail and More Effective Threat Impact Analysis

Sourcefire & Qualys Integration Highlights

Benefits

- Provides additional contextual network detail
- Provides more effective impact analysis
- Expands impact analysis to network segments not yet monitored by Sourcefire RNA
- Extends your investment in your current solution
- Improves network security

Qualys Integration Service from Sourcefire

- Available with Sourcefire 3D System 4.8 & beyond
- Integration software provided by Sourcefire Professional Services
  - » 3 or 5 days of remote set-up services
  - » Onsite options also available

When your network is under attack, you need as much contextual data about your network as you can possibly get. Contextual network data—information about the composition of the hosts on your networks and the applications that these hosts are running—helps security analysts prioritize intrusion alerts and gauge their malicious intent, making the analysts more effective. Sourcefire RNA® (Real-time Network Awareness) provides valuable network context, and QualysGuard® Vulnerability Management (VM) supplies additional contextual data for more effective threat impact analysis.

The integration between Sourcefire and Qualys consists of importing a customer's QualysGuard vulnerability data into the Sourcefire 3D® System, leveraging Sourcefire Defense Center® to correlate threats detected by Sourcefire IPS™ (Intrusion Prevention System) against host vulnerabilities identified by QualysGuard VM. With Sourcefire and Qualys working in tandem, an organization receives more effective threat impact analysis that covers a wider range of vulnerabilities across more applications, extending your current investment and increasing security.

A CLOSER LOOK AT QUALYSGUARD VM

QualysGuard VM automates the lifecycle of network auditing and vulnerability management across the enterprise, including network discovery and mapping, asset prioritization, vulnerability assessment reporting, and remediation tracking according to business risk. QualysGuard VM allows security managers to audit, enforce, and document network security in accordance with internal policies and external regulations. As an on-demand Software-as-a-Service (SaaS) solution, there is no infrastructure to deploy or manage.

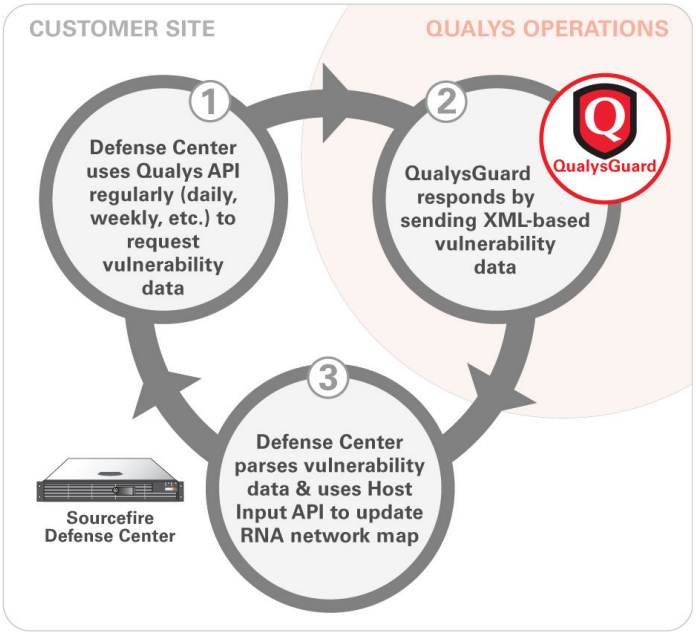
QualysGuard VM enables enterprises to effectively manage their vulnerabilities and maintain control over their network security with centralized reports, verified remedies, and full remediation workflow capabilities with trouble tickets. QualysGuard provides comprehensive reports on vulnerabilities including severity levels, time-to-fix estimates, and impact on business, plus trend analysis on security issues.

THE BEST OF BOTH WORLDS: COMBINING ACTIVE AND PASSIVE VULNERABILITY ANALYSIS

Active vulnerability scanning and passive vulnerability analysis each have their advantages. Active scanning provides more accurate vulnerability data because the existence of each vulnerability has been verified, while passive analysis offers 24-hour coverage of your network between active scans. Sourcefire RNA is a passive network intelligence solution that stores a real-time inventory of operating systems, services, applications, and potential vulnerabilities that exist on your network. By combining QualysGuard's active vulnerability scan data with Sourcefire RNA's passive sensing technology, your organization gets the best of both worlds.

Using the Sourcefire Host Input API, the Sourcefire and Qualys integration provides customers with the ability to import QualysGuard scan data into the RNA host database. By correlating threats against QualysGuard vulnerabilities, an Impact Flag 1 event depicts a host that is vulnerable to the associated exploit. Through this combination of Sourcefire's real-time

network discovery information with QualysGuard's vulnerability scan data, an organization receives more effective impact analysis covering a wider range of vulnerabilities across more applications.



THE BENEFITS OF IMPACT ANALYSIS WITH QUALYSGUARD AND SOURCEFIRE RNA VULNERABILITIES

Sourcefire customers can now correlate IPS intrusion events with QualysGuard vulnerabilities, signifying high impact events when QualysGuard identifies a host as being vulnerable to a network threat. The Sourcefire and Qualys integration provides significant benefits, including:

- Additional contextual network detail and more effective impact analysis
- Impact analysis expanded to segments of your network not yet monitored by RNA
- Extension of your investment in your current solution and improved network security

A key benefit of the Sourcefire and Qualys integration is that it provides more contextual detail about a network and improves the effectiveness of impact analysis. Qualys vulnerability data may include vulnerabilities for applications that RNA may not detect. RNA detects many applications, but there are some applications that Qualys can detect but RNA cannot, and vice versa. Adding these Qualys-specific vulnerabilities to the Sourcefire 3D System means that impact analysis will be more effective and cover a wider range of vulnerabilities across more applications.

For example, an intrusion event may reference a vulnerability in an application that RNA does not detect. The 3D System is not aware of the application or the application's vulnerabilities, so it will set the Impact Flag to "Potentially Vulnerable" or "Not Vulnerable". If QualysGuard vulnerability data identifies the event's targeted host as vulnerable and this vulnerability is already in the Sourcefire vulnerability database (VDB), then the intrusion event will have an Impact Flag of "Vulnerable" because the 3D System is now aware of the host's vulnerability. A secondary benefit of the Sourcefire and Qualys integration is that users may expand impact analysis to segments of the network not

yet monitored by RNA. For example, a large, distributed organization may use Qualys to scan hosts in multiple remote sites, but it may not yet have deployed RNA to these sites for cost, time, or management reasons. This organization could import the Qualys vulnerability data for these remote hosts into the 3D System, and impact analysis would be able to correlate against the vulnerabilities found for these hosts.

TAKE THE NEXT STEP TO PROTECT YOUR NETWORK

The Sourcefire and Qualys integration is available with Sourcefire 3D System 4.8 and beyond, and Sourcefire Professional Services provides the integration software as part of its Qualys Integration Service. The service provides either three or five days of remote set-up service, but onsite options are also available.

Learn more about how you can benefit from the combination of leading technology from Sourcefire and Qualys. Visit us at www.sourcefire.com or contact Sourcefire or a Sourcefire reseller to learn more about the Qualys Integration Service.