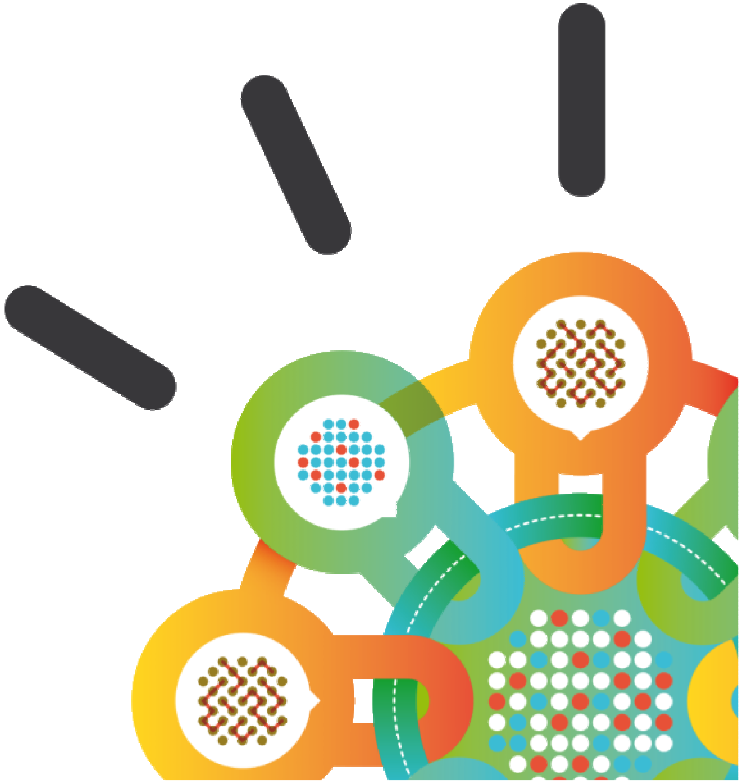
QRadar Vulnerability Manager v7.2.2
QRadar Risk Manager v7.2.2

New Feature Overview

April 2014



New capabilities!

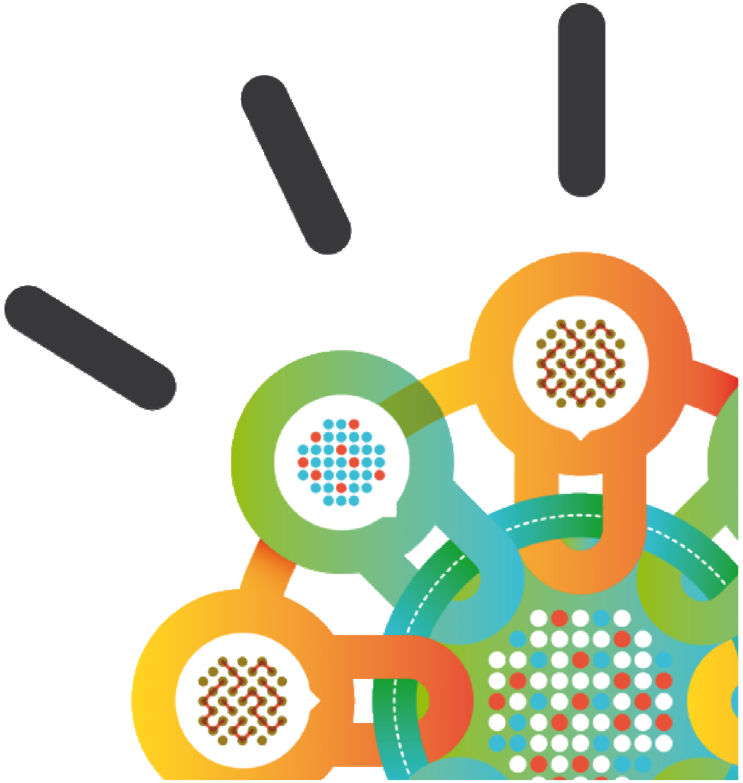
- QRadar Vulnerability Manager
  - New capabilities deliver even more value, improve usability and scalability
  - Scan policies reduce scan time, increase performance and flexibility
  - Centralized credentials reduce administration time and overhead
  - Automatic scanner assignment increases scalability, eases administration
  - Asset owner management streamlines en masse owner changes
  - Scheduled scan views enables visualization of scheduled scans, eliminating potential overlaps and improving scan efficiencies
  - Enhanced reporting capabilities

    PCI ASV, risk prioritized remediation and asset reports and much more!

- QRadar Risk Manager
  - Drastically improved topology performance scales to even larger environments
  - New policy tests enable complex Windows configuration policies like CIS
  - Support for new IPS and Next Gen firewall devices expands topology and policy capabilities
  - Improved path visualizations decrease network administration overhead for users

QRadar Vulnerability Manager v7.2.2

New Feature Overview



- Improved usability and scan performance

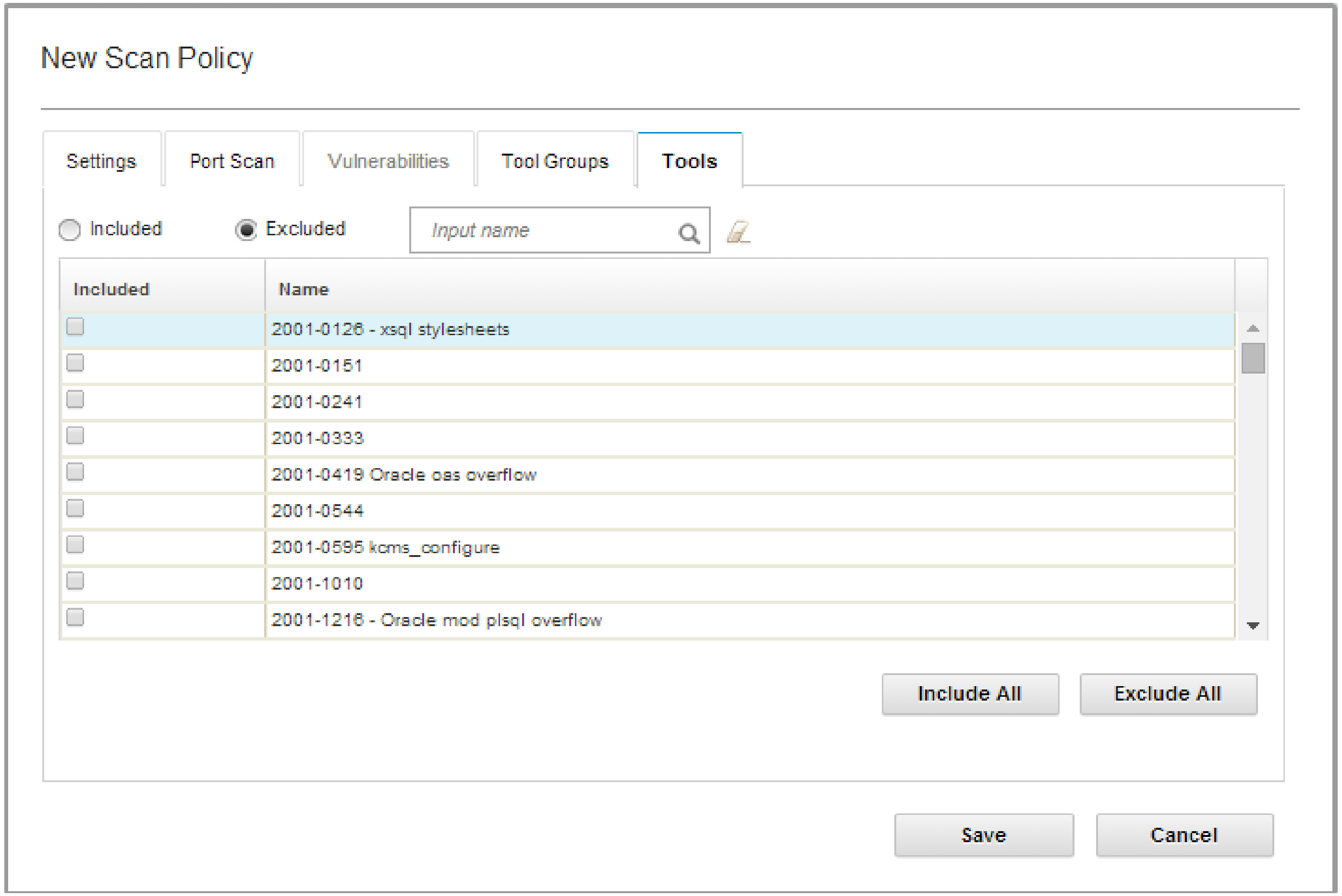
- Scan Policies
- Dynamic Scanning
- Automated asset owner assignment

Scan policies enable focused, rapid scanning

- Customers can now granularly configure the way that QRadar Vulnerability Manager scans assets through scan policies
- This improves scan performance by reducing the total number of scan tests conducted
  - Example: turn off scans for vulnerabilities that are 10+ years old
- This also allows customers to selectively turn specific vulnerability tests on and off, giving them a high degree of control over how their assets are scanned
- QVM customers can now define their own scan policies, which includes selecting / deselecting specific tests, for virtually any scan type:
  - Full scan
  - Database scan
  - Discovery scan
  - PCI scan
  - Patch scan
  - Web scan
- Patch scan policies may also include specific vulnerabilities to check for
  - Enables rapid scanning for specific vulnerabilities (e.g. heartbleed); vulnerabilities may be quickly selected via quick filter

Scan policy example

- Scan policy that excludes thousands of old vulnerabilities from 2001



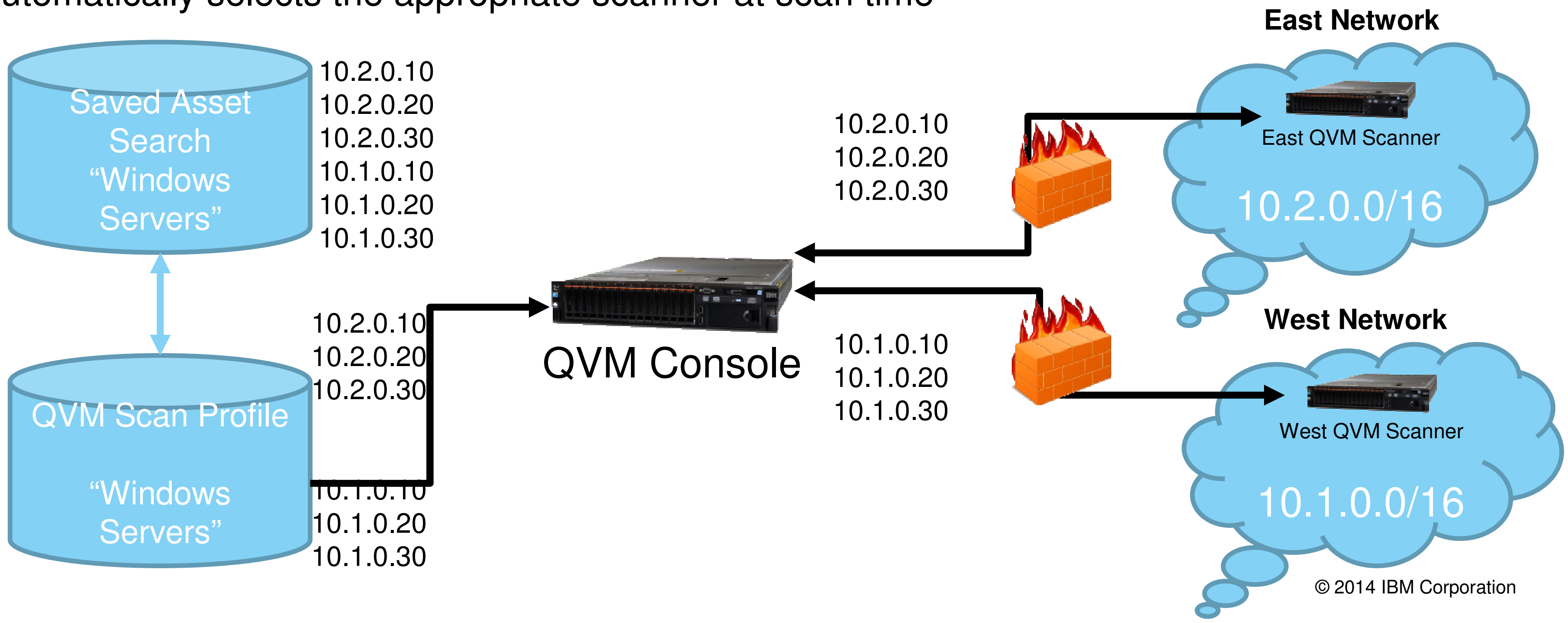
New Scan Policy

○ Included ● Excluded

Included	Name
□	2001-0126 - xsql stylesheets
□	2001-0151
□	2001-0241
□	2001-0333
□	2001-0419 Oracle oas overflow
□	2001-0544
□	2001-0595 kcms_configure
□	2001-1010
□	2001-1216 - Oracle mod plsql overflow

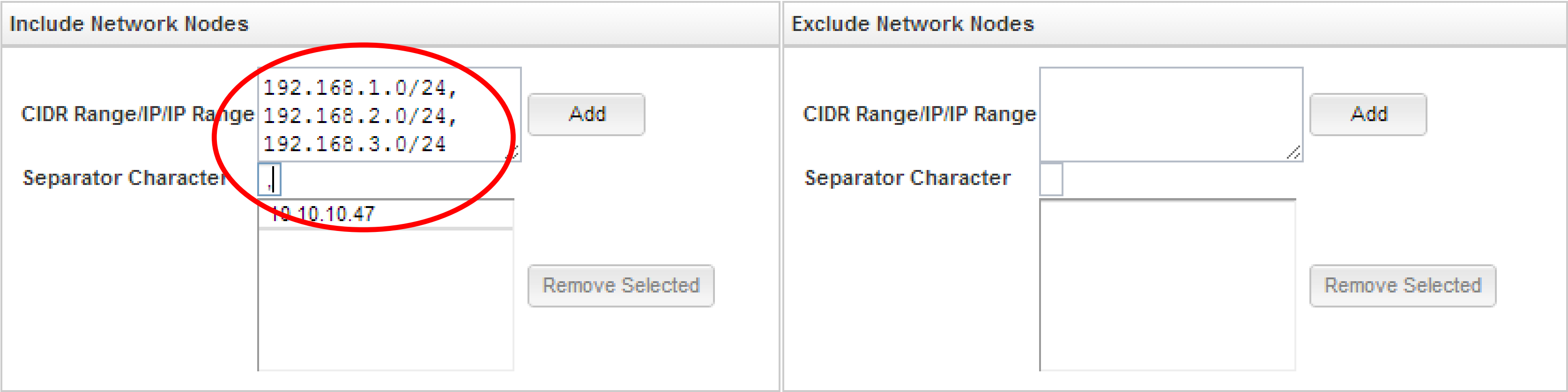
Dynamic scanning allows automatic selection of the appropriate scanner

- Dynamic scanning allows QVM users to assign ranges of IPs to specific QVM scanners
- Previously, QVM scans were limited to one scanner per scan profile
  - For example, users create a saved asset search to cover all Windows servers
  - QVM scan profile was created, specifying the saved asset search
  - The scan profile was limited to a single scanner, so selection of the "best" scanner to cover all IPs was not possible
- Users can now assign specific CIDR or IP ranges to specific scanners; QVM then automatically selects the appropriate scanner at scan time



Simplifying the definition of large scans

- QVM now allows users to copy and paste a delimited list of IP addresses into the QVM scan profile, specifying the separator character
- Many customers store asset information in delimited format (like CSV); QVM now simplifies the process of copying that information into the scan profile



Include Network Nodes

CIDR Range/IP/IP Range: 192.168.1.0/24, 192.168.2.0/24, 192.168.3.0/24

Separator Character: ,

10.10.10.47

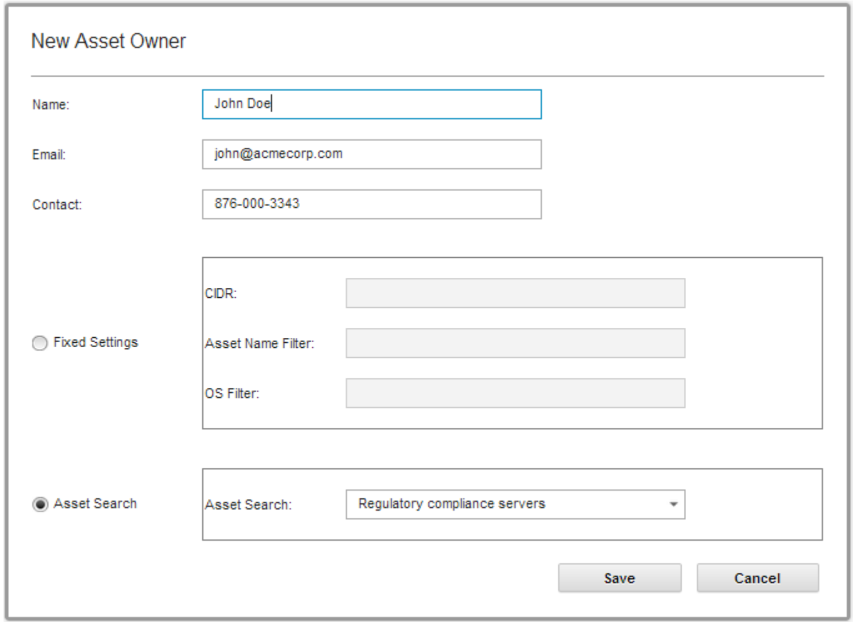
Exclude Network Nodes

CIDR Range/IP/IP Range

Separator Character

Automated asset owner assignment eases administration for large customers

- QVM relies on the technical owner name and contact information in the asset database to assign vulnerabilities to users and automatically distribute reports via email
- Users need the ability to assign technical user and contact information to many assets en masse; also allows easy reassignment
- Asset owners may be assigned by CIDR, name, OS, or via saved asset search
- Remediation deadlines by owner and scheduled assignment runs may also be set



New Asset Owner

Name: John Doe

Email: john@acmecorp.com

Contact: 876-000-3343

○ Fixed Settings

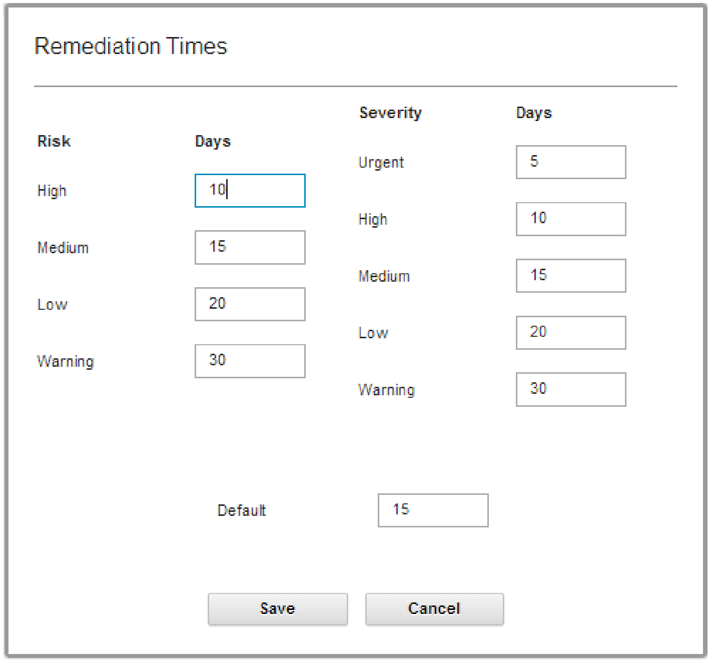
CIDR:

Asset Name Filter:

OS Filter:

● Asset Search

Asset Search: Regulatory compliance servers



Remediation Times

Risk	Days	Severity	Days
High	10	Urgent	5
Medium	15	High	10
Low	20	Medium	15
Warning	30	Low	20
		Warning	30

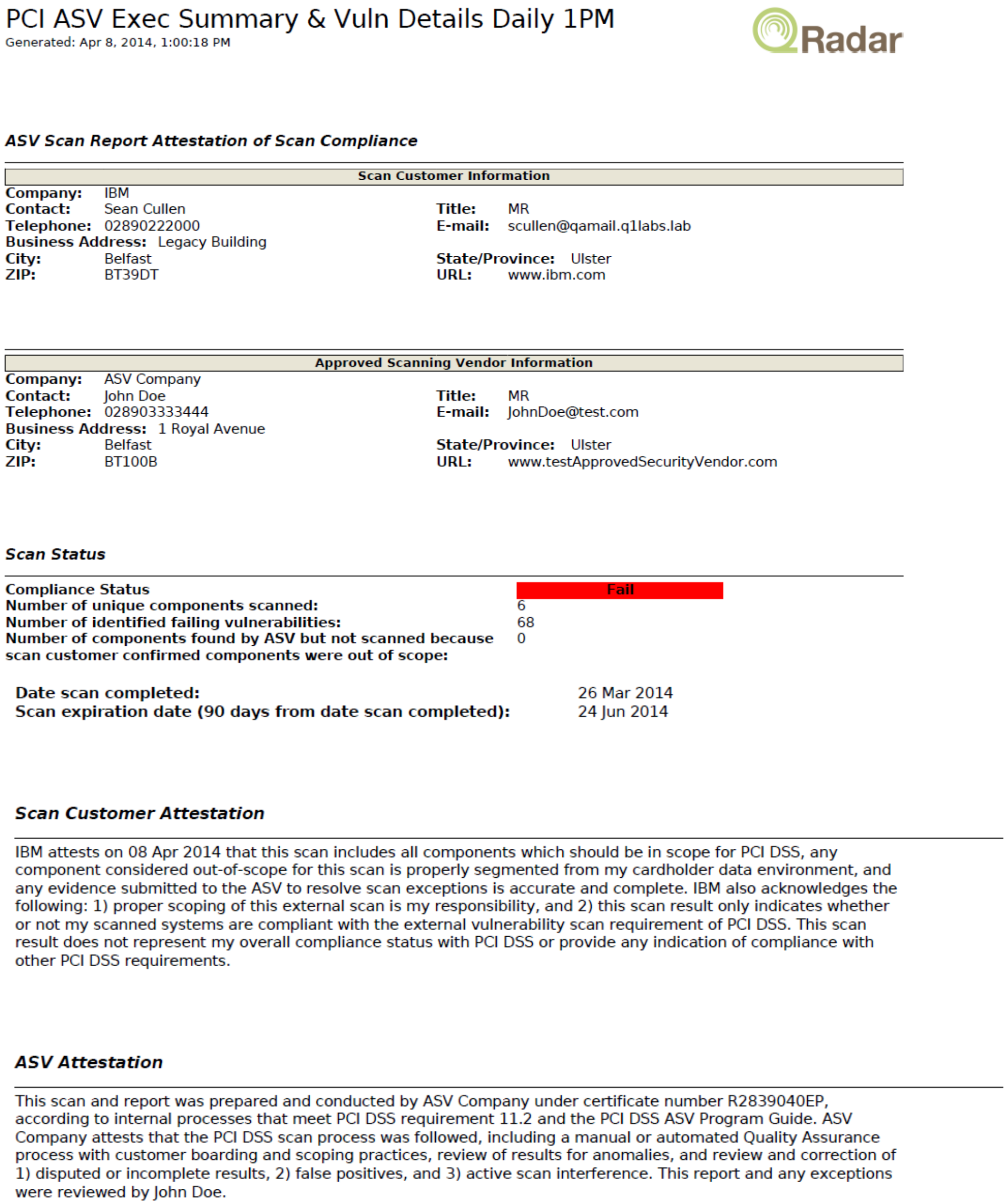
Default 15

- Intelligence driven remediation and compliance efficiency improvements

Intelligence driven remediation and compliance efficiency improvements

- A key advantage of QVM+QRM is risk prioritization of remediation and compliance processes
  - For example, QRM policies can increase and decrease vulnerability risk scores based on factors including correlation of asset communications, network reachability, asset configuration, patch status, etc
  - This applies to virtually all vulnerabilities, including those acquired from AppScan, IEM/BigFix, Guardium, and third party vulnerability scanners
- Addition of many new out-of-the-box reports, coupled with risk scoring, provide functionality not found in any other product on the market
  - Automated creation and distribution of risk-prioritized patching, vulnerabilities, and asset reports is a huge competitive advantage!
  - Examples
    - PCI ASV report: PCI Approved Scanning Vendors will be able to use QVM to scan customer networks and “attest” to compliance with PCI standards; QRadar customers can run their own tests to ensure that they will pass ASV scans
      QVM PCI ASV report is in the process of being certified by PCI; Q2 2014 target
    - Generation and distribution of risk prioritized compliance, asset, patch reports
    - “Reminder” reports for asset owners, by assignee, root cause, asset patch, vulnerability asset, asset OS patches, etc

PCI ASV Report



PCI ASV Exec Summary & Vuln Details Daily 1PM

Generated: Apr 8, 2014, 1:00:18 PM

ASV Scan Report Attestation of Scan Compliance

Scan Customer Information

Company:	IBM		
Contact:	Sean Cullen	**Title:**	MR
Telephone:	02890222000	**E-mail:**	scullen@qamail.q1labs.lab
Business Address:	Legacy Building		
City:	Belfast	**State/Province:**	Ulster
ZIP:	BT39DT	**URL:**	www.ibm.com

Approved Scanning Vendor Information

Company:	ASV Company		
Contact:	John Doe	**Title:**	MR
Telephone:	028903333444	**E-mail:**	JohnDoe@test.com
Business Address:	1 Royal Avenue		
City:	Belfast	**State/Province:**	Ulster
ZIP:	BT100B	**URL:**	www.testApprovedSecurityVendor.com

Scan Status

Compliance Status	Fail
Number of unique components scanned:	6
Number of identified failing vulnerabilities:	68
Number of components found by ASV but not scanned because scan customer confirmed components were out of scope:	0

Date scan completed:	26 Mar 2014
Scan expiration date (90 days from date scan completed):	24 Jun 2014

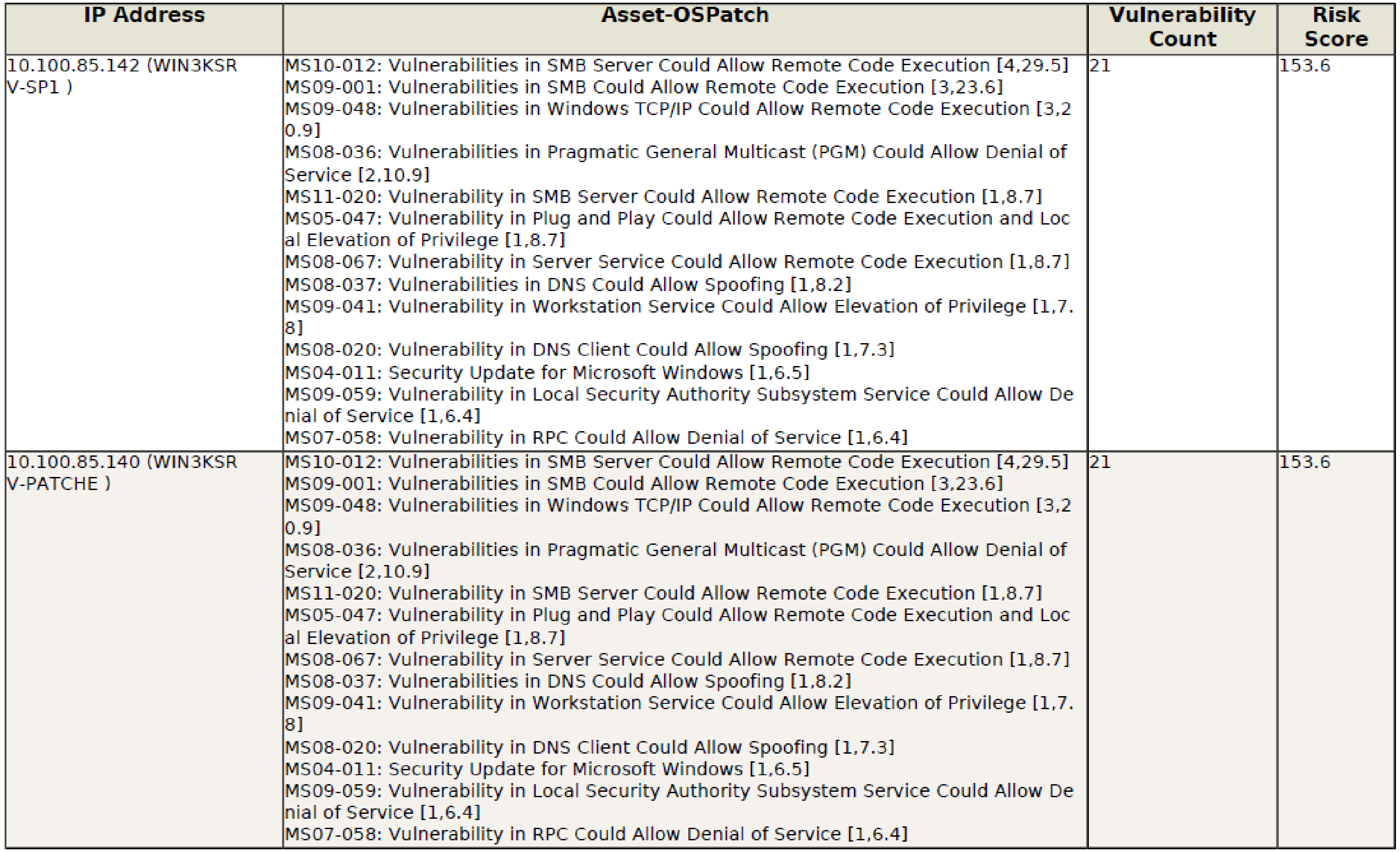
Scan Customer Attestation

IBM attests on 08 Apr 2014 that this scan includes all components which should be in scope for PCI DSS, any component considered out-of-scope for this scan is properly segmented from my cardholder data environment, and any evidence submitted to the ASV to resolve scan exceptions is accurate and complete. IBM also acknowledges the following: 1) proper scoping of this external scan is my responsibility, and 2) this scan result only indicates whether or not my scanned systems are compliant with the external vulnerability scan requirement of PCI DSS. This scan result does not represent my overall compliance status with PCI DSS or provide any indication of compliance with other PCI DSS requirements.

ASV Attestation

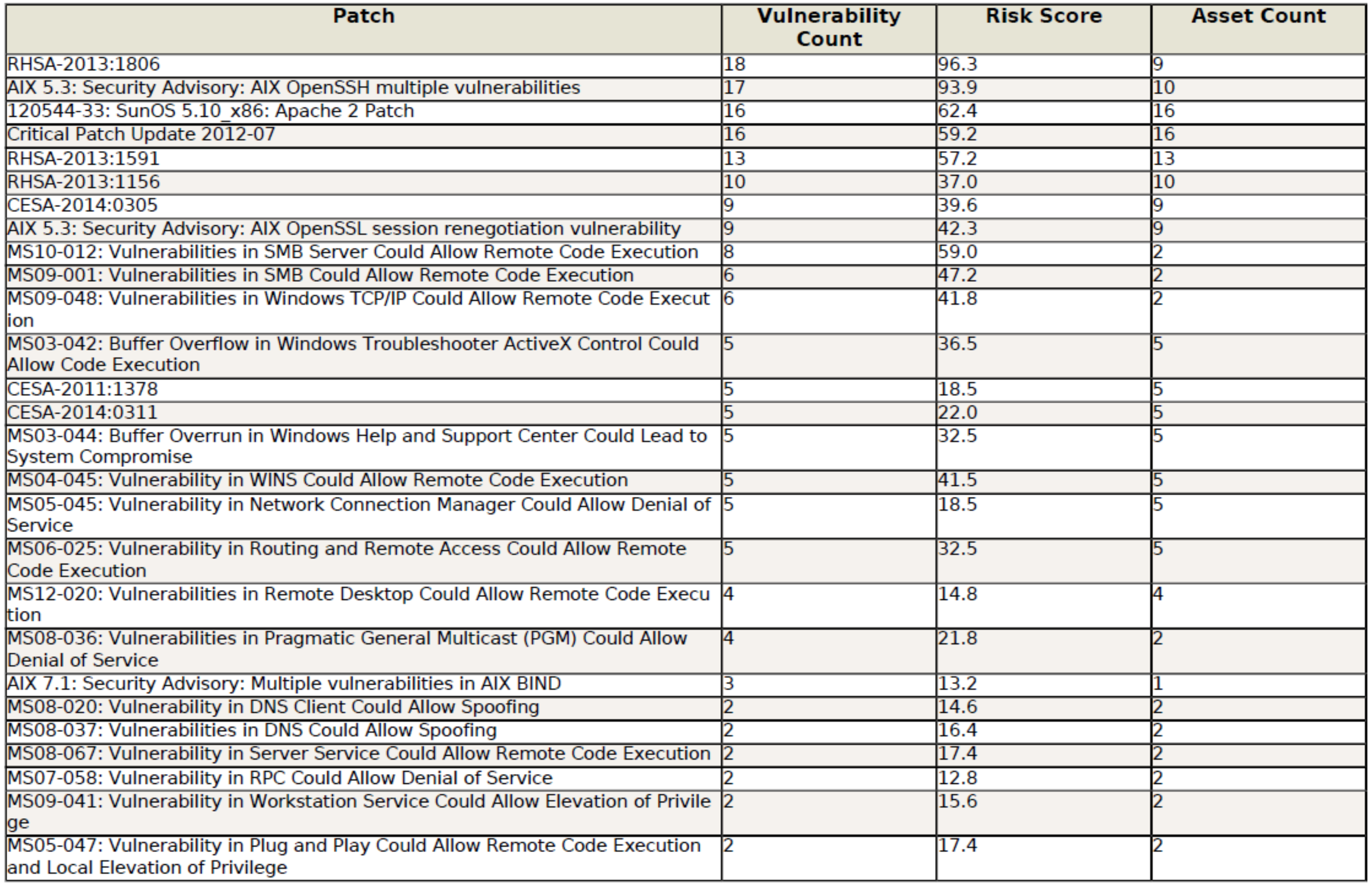
This scan and report was prepared and conducted by ASV Company under certificate number R2839040EP, according to internal processes that meet PCI DSS requirement 11.2 and the PCI DSS ASV Program Guide. ASV Company attests that the PCI DSS scan process was followed, including a manual or automated Quality Assurance process with customer boarding and scoping practices, review of results for anomalies, and review and correction of 1) disputed or incomplete results, 2) false positives, and 3) active scan interference. This report and any exceptions were reviewed by John Doe.

Assets and patches prioritized by risk allow customers to remediate riskiest assets first



IP Address	Asset-OSPatch	Vulnerability Count	Risk Score
10.100.85.142 (WIN3KSRV-SP1)	MS10-012: Vulnerabilities in SMB Server Could Allow Remote Code Execution [4,29.5] MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution [3,23.6] MS09-048: Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution [3,20.9] MS08-036: Vulnerabilities in Pragmatic General Multicast (PGM) Could Allow Denial of Service [2,10.9] MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution [1,8.7] MS05-047: Vulnerability in Plug and Play Could Allow Remote Code Execution and Local Elevation of Privilege [1,8.7] MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution [1,8.7] MS08-037: Vulnerabilities in DNS Could Allow Spoofing [1,8.2] MS09-041: Vulnerability in Workstation Service Could Allow Elevation of Privilege [1,7.8] MS08-020: Vulnerability in DNS Client Could Allow Spoofing [1,7.3] MS04-011: Security Update for Microsoft Windows [1,6.5] MS09-059: Vulnerability in Local Security Authority Subsystem Service Could Allow Denial of Service [1,6.4] MS07-058: Vulnerability in RPC Could Allow Denial of Service [1,6.4]	21	153.6
10.100.85.140 (WIN3KSRV-PATCHE)	MS10-012: Vulnerabilities in SMB Server Could Allow Remote Code Execution [4,29.5] MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution [3,23.6] MS09-048: Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution [3,20.9] MS08-036: Vulnerabilities in Pragmatic General Multicast (PGM) Could Allow Denial of Service [2,10.9] MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution [1,8.7] MS05-047: Vulnerability in Plug and Play Could Allow Remote Code Execution and Local Elevation of Privilege [1,8.7] MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution [1,8.7] MS08-037: Vulnerabilities in DNS Could Allow Spoofing [1,8.2] MS09-041: Vulnerability in Workstation Service Could Allow Elevation of Privilege [1,7.8] MS08-020: Vulnerability in DNS Client Could Allow Spoofing [1,7.3] MS04-011: Security Update for Microsoft Windows [1,6.5] MS09-059: Vulnerability in Local Security Authority Subsystem Service Could Allow Denial of Service [1,6.4] MS07-058: Vulnerability in RPC Could Allow Denial of Service [1,6.4]	21	153.6

Patches prioritized by vulnerability count allow customers to determine which patches to apply first



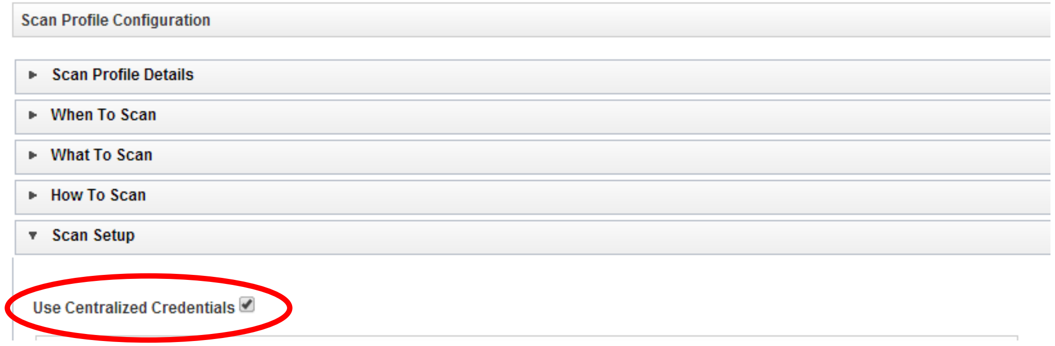
Patch	Vulnerability Count	Risk Score	Asset Count
RHSA-2013:1806	18	96.3	9
AIX 5.3: Security Advisory: AIX OpenSSH multiple vulnerabilities	17	93.9	10
120544-33: SunOS 5.10_x86: Apache 2 Patch	16	62.4	16
Critical Patch Update 2012-07	16	59.2	16
RHSA-2013:1591	13	57.2	13
RHSA-2013:1156	10	37.0	10
CESA-2014:0305	9	39.6	9
AIX 5.3: Security Advisory: AIX OpenSSL session renegotiation vulnerability	9	42.3	9
MS10-012: Vulnerabilities in SMB Server Could Allow Remote Code Execution	8	59.0	2
MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution	6	47.2	2
MS09-048: Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution	6	41.8	2
MS03-042: Buffer Overflow in Windows Troubleshooter ActiveX Control Could Allow Code Execution	5	36.5	5
CESA-2011:1378	5	18.5	5
CESA-2014:0311	5	22.0	5
MS03-044: Buffer Overrun in Windows Help and Support Center Could Lead to System Compromise	5	32.5	5
MS04-045: Vulnerability in WINS Could Allow Remote Code Execution	5	41.5	5
MS05-045: Vulnerability in Network Connection Manager Could Allow Denial of Service	5	18.5	5
MS06-025: Vulnerability in Routing and Remote Access Could Allow Remote Code Execution	5	32.5	5
MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution	4	14.8	4
MS08-036: Vulnerabilities in Pragmatic General Multicast (PGM) Could Allow Denial of Service	4	21.8	2
AIX 7.1: Security Advisory: Multiple vulnerabilities in AIX BIND	3	13.2	1
MS08-020: Vulnerability in DNS Client Could Allow Spoofing	2	14.6	2
MS08-037: Vulnerabilities in DNS Could Allow Spoofing	2	16.4	2
MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution	2	17.4	2
MS07-058: Vulnerability in RPC Could Allow Denial of Service	2	12.8	2
MS09-041: Vulnerability in Workstation Service Could Allow Elevation of Privilege	2	15.6	2
MS05-047: Vulnerability in Plug and Play Could Allow Remote Code Execution and Local Elevation of Privilege	2	17.4	2

- Making QVM even easier to use

- Centralized credential management
- Scheduled scan views

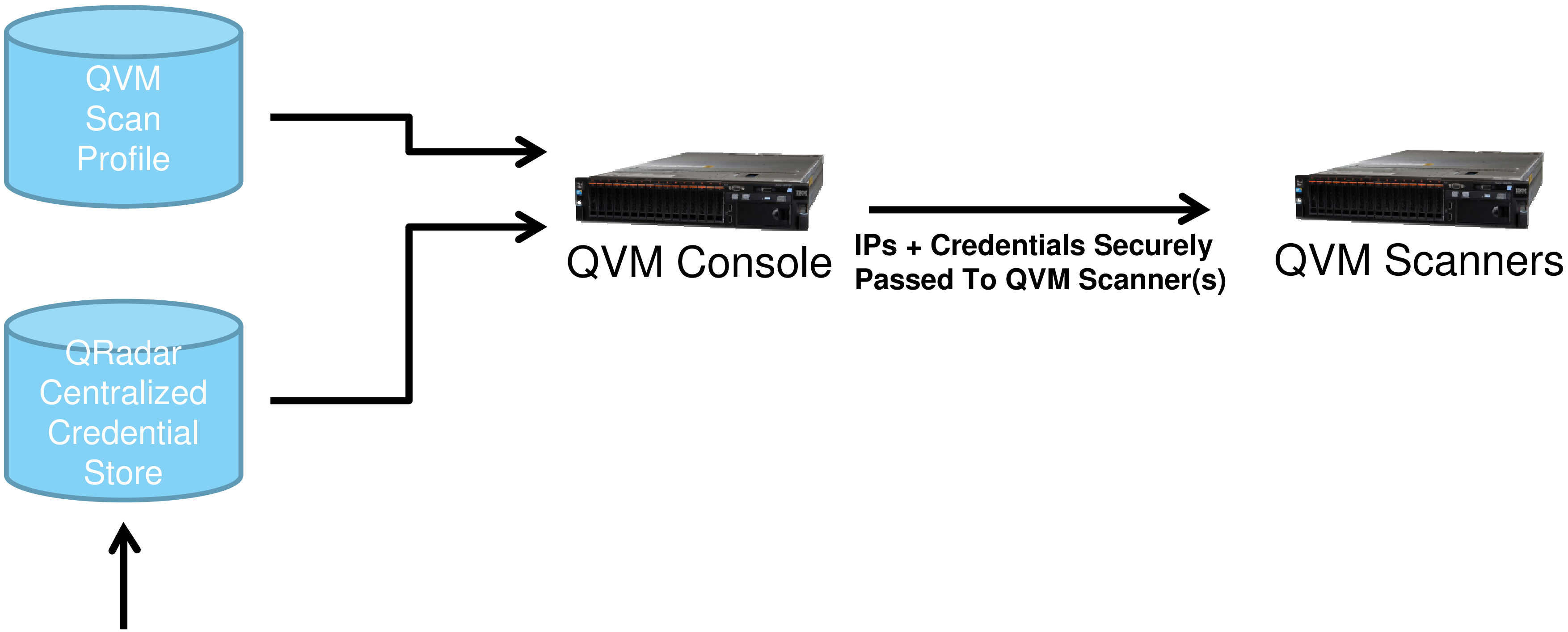
Centralized credentials streamlines administration, enables separation of duties

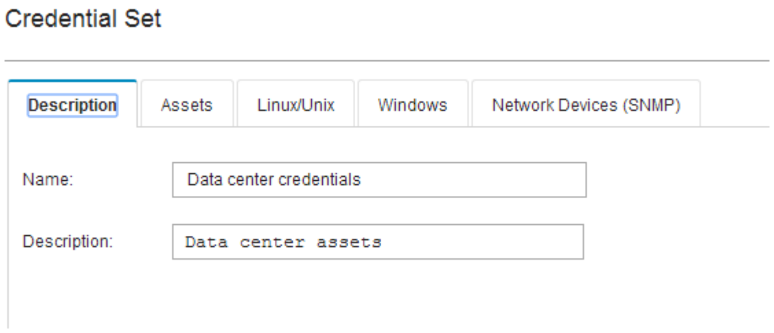
- QRadar Vulnerability Manager now allows users to specify vulnerability scan credentials in each scan profile or via a secure centralized credentials facility
- Credentials can be selectively applied to scan profiles, simplifying administration and enabling separation of duties
  - People scheduling scans don’t need credentials for the machines being scanned
  - Eases credential definition for on-demand and rule-driven scans
- Users create credential sets via the QRadar admin tab, specifying CIDRs covered by the credentials
  - Centralized credentials utility can be utilized by other QRadar modules in the future
- Credentials are then entered for Windows, Linux/UNIX and network (SNMP) devices
- When users create QVM scan profile, they check ‘use centralized credentials’, which instructs QVM to pull credentials from the CC store at scan time



Use Centralized Credentials ☑

Centralized credentials

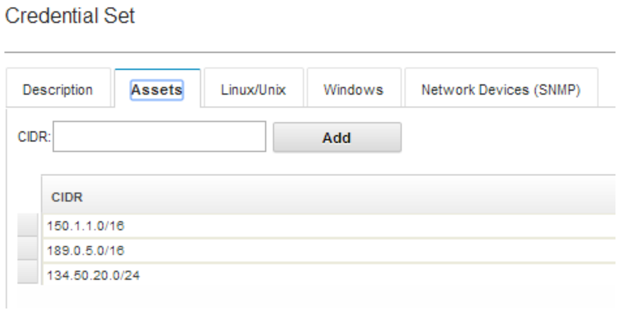

QVM Scan Profile
QRadar Centralized Credential Store
QVM Console
IPs + Credentials Securely Passed To QVM Scanner(s)
QVM Scanners



Credential Set

Name: Data center credentials

Description: Data center assets



Credential Set

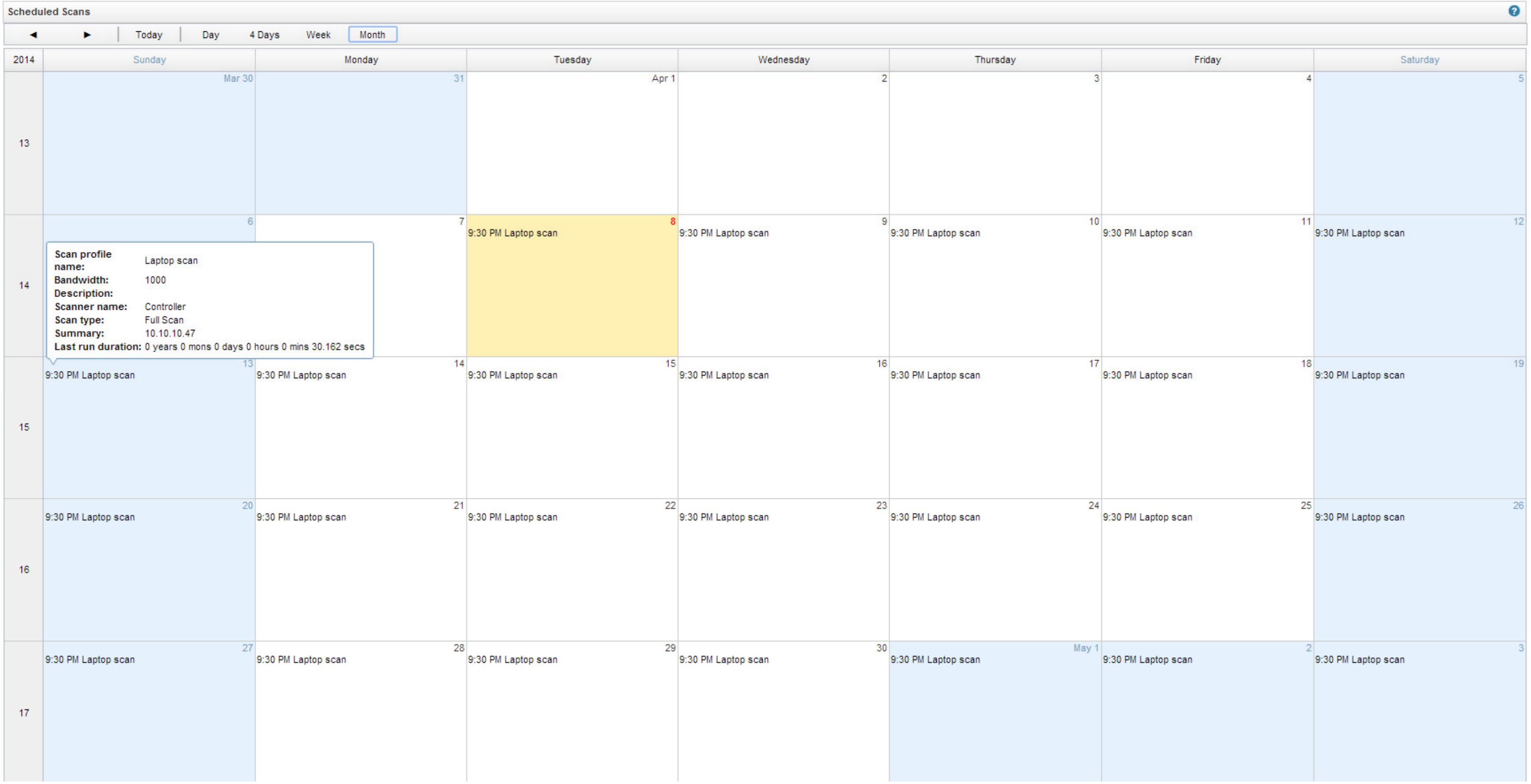
CIDR:

CIDR
150.1.1.0/16
189.0.5.0/16
134.50.20.0/24

Centralized Credentials

Scheduled scan views help avoid overlaps, minimize network and asset traffic

- Users can now view which scans are scheduled to run on a daily, weekly, and monthly basis
- Views also graphically display last scan duration; scans profiles may also be edited directly from calendar views



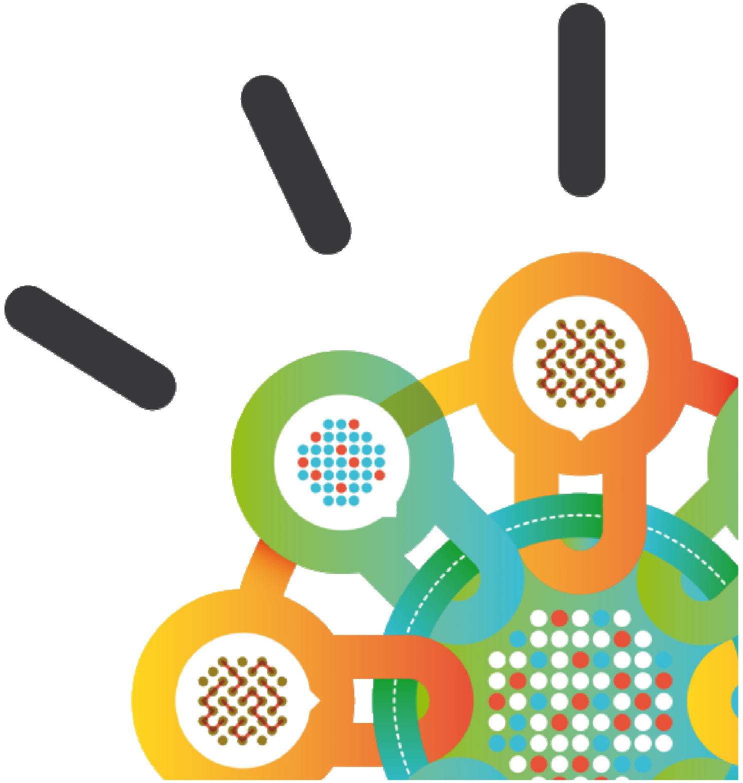
Scheduled Scans

2014	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
13	Mar 30	31	Apr 1	2	3	4	5
14	6	7	8 9:30 PM Laptop scan	9 9:30 PM Laptop scan	10 9:30 PM Laptop scan	11 9:30 PM Laptop scan	12 9:30 PM Laptop scan
15	13 9:30 PM Laptop scan	14 9:30 PM Laptop scan	15 9:30 PM Laptop scan	16 9:30 PM Laptop scan	17 9:30 PM Laptop scan	18 9:30 PM Laptop scan	19 9:30 PM Laptop scan
16	20 9:30 PM Laptop scan	21 9:30 PM Laptop scan	22 9:30 PM Laptop scan	23 9:30 PM Laptop scan	24 9:30 PM Laptop scan	25 9:30 PM Laptop scan	26 9:30 PM Laptop scan
17	27 9:30 PM Laptop scan	28 9:30 PM Laptop scan	29 9:30 PM Laptop scan	30 9:30 PM Laptop scan	May 1 9:30 PM Laptop scan	2 9:30 PM Laptop scan	3 9:30 PM Laptop scan

Scan profile name:	Laptop scan
Bandwidth:	1000
Description:	
Scanner name:	Controller
Scan type:	Full Scan
Summary:	10.10.10.47
Last run duration:	0 years 0 mons 0 days 0 hours 0 mins 30.162 secs

QRadar Risk Manager v7.2.2

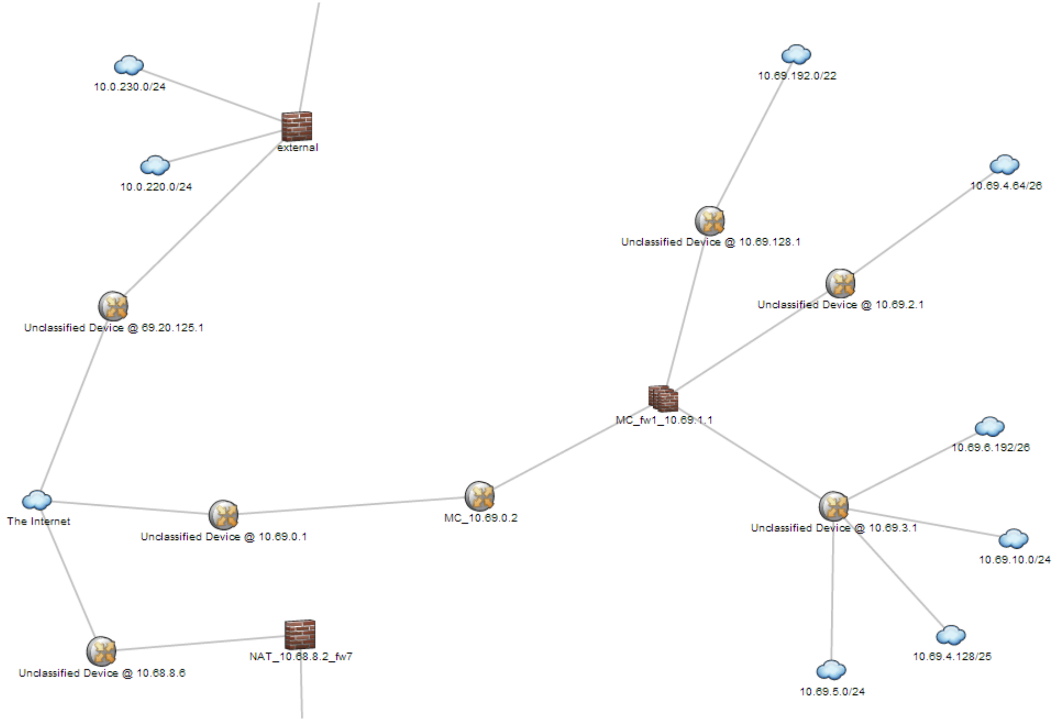
New Feature Overview



- Improved QRM performance, scalability and usability
- New topology model
- Complex configuration tests and compliance standard support
- New device support
- Improved path searching

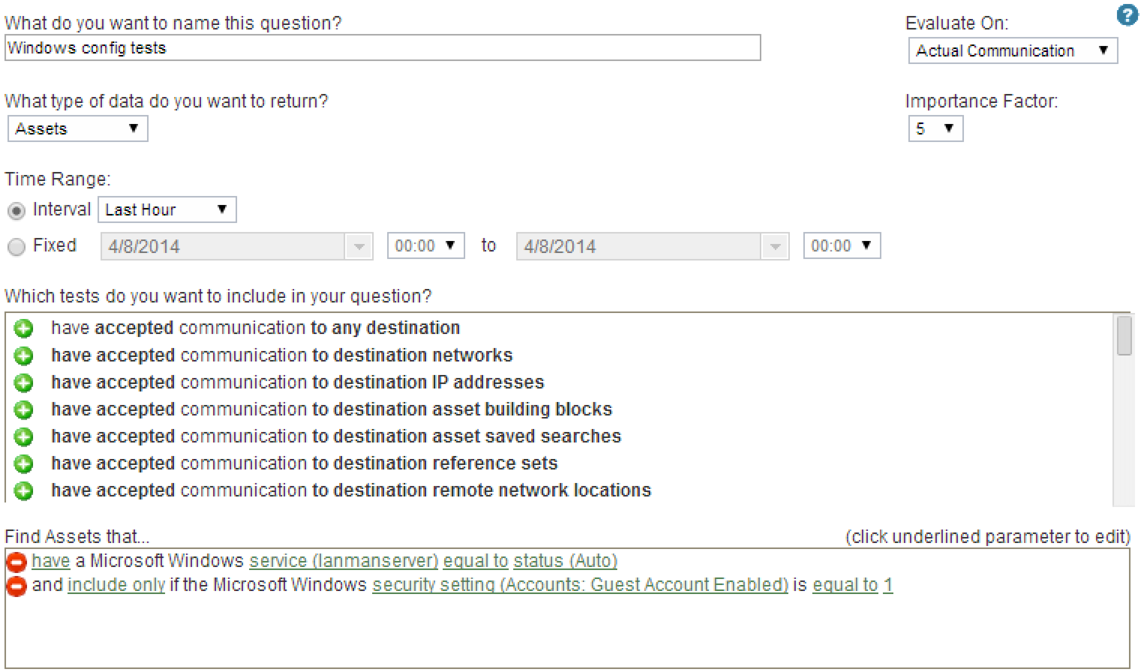
New QRM topology model provides drastically faster performance, scalability

- Performing topology calculations in large, complex customer networks could be time and resource intensive
- A new approach to topology calculations now uses set arithmetic and geometric shapes, combined with improved multi-threading, dramatically improves performance and scalability
  - Initial benchmarks show 600% to 700% topology calculation performance gains
  - This will allow QRM to support large customers with > 10,000 devices and will set the stage for near time-time topology and risk calculations as customer network configurations change


10.0.230.0/24
external
10.0.220.0/24
Unclassified Device @ 69.20.125.1
The Internet
Unclassified Device @ 10.69.0.1
MC_10.69.0.2
Unclassified Device @ 10.68.8.6
NAT_10.68.8.2_fw7
10.69.192.0/22
Unclassified Device @ 10.69.128.1
10.69.4.64/26
Unclassified Device @ 10.69.2.1
MC_fw1_10.69.1.1
10.69.6.192/26
Unclassified Device @ 10.69.3.1
10.69.10.0/24
10.69.4.128/25
10.69.5.0/24

New policy monitor tests support complex configuration tests and compliance standards

- QRadar Risk Manager policy monitor test mechanism has been improved, removing requirement for additive communications tests and increasing test flexibility
- Improved policy monitor tests
  - Windows configuration tests can now be additive; Windows property tests can be ‘equal’ or ‘not equal’; multiple configuration tests can be included in a single policy
- These changes are required in order to support configuration-based compliance policies
- Examples: CIS benchmarks, enforcing corporate configuration standards



What do you want to name this question?
Windows config tests

Evaluate On:
Actual Communication ▼

What type of data do you want to return?
Assets ▼

Importance Factor:
5 ▼

Time Range:
● Interval Last Hour ▼
○ Fixed 4/8/2014 00:00 ▼ to 4/8/2014 00:00 ▼

Which tests do you want to include in your question?
- have accepted communication to any destination
- have accepted communication to destination networks
- have accepted communication to destination IP addresses
- have accepted communication to destination asset building blocks
- have accepted communication to destination asset saved searches
- have accepted communication to destination reference sets
- have accepted communication to destination remote network locations

Find Assets that... (click underlined parameter to edit)

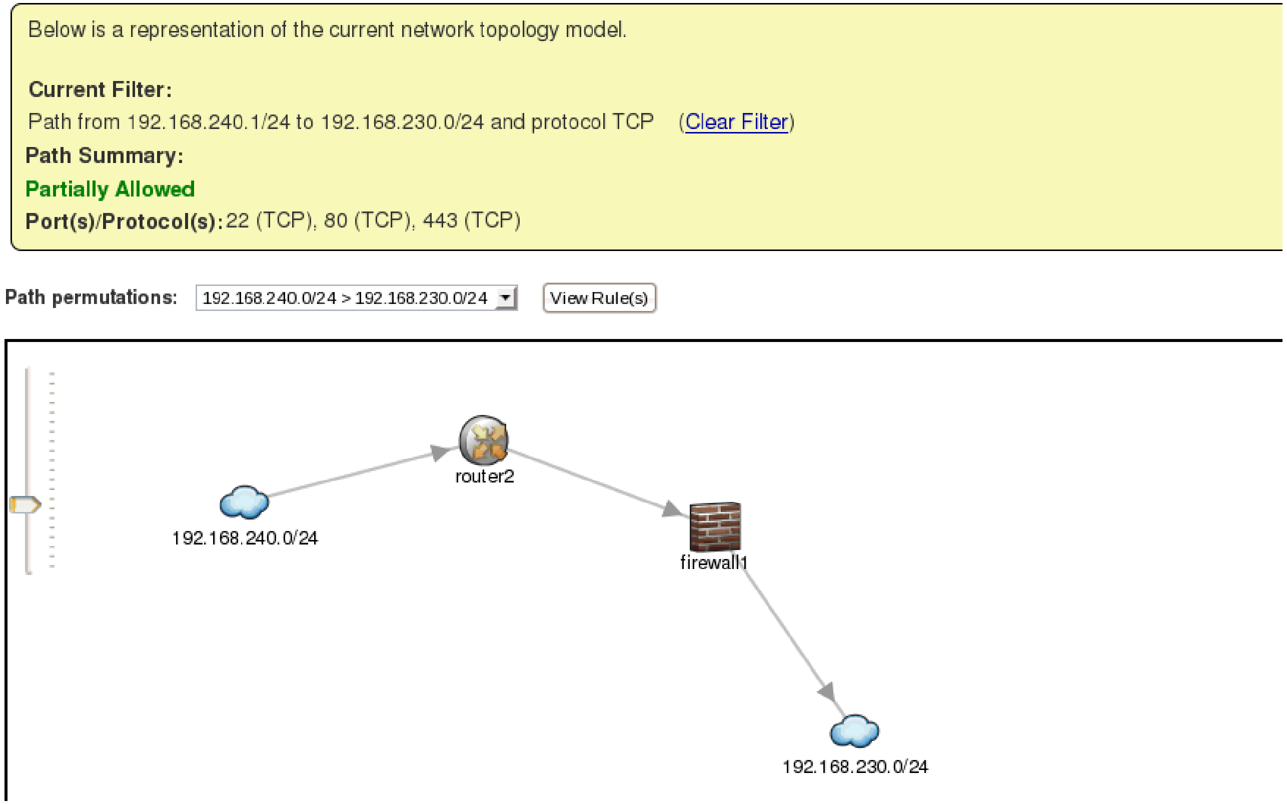
have a Microsoft Windows service (lanmanserver) equal to status (Auto)
and include only if the Microsoft Windows security setting (Accounts: Guest Account Enabled) is equal to 1

New IPS and NextGen firewall support extends topology and policy coverage

- Support for “next generation”, “application layer”, and “layer 7” devices, which function at the application level, is being added to QRM this year in phases
  - This includes firewalls and intrusion prevention systems (IPS)
    - Examples: Palo Alto Networks, Juniper Networks SRX, IBM XGS IPS, Sourcefire IPS, Tipping Point IPS, etc.
  - Support for these devices provides many advantages
    - Policy monitor tests that correlate vulnerabilities with network reachability will take these devices into account
    - Ability to view device configurations and track historical configuration changes
- Phased approach
  1. QRM 7.2.2: layer 3 support
     - Collection of device configuration data
     - Placement of devices in topology
  2. QRM 7.2.3 and 7.2.4: layer 7 (application) support
     - Full support for layer 7 (application) configurations
     - Additional policy monitor tests to support application layer communication and exploitability tests
- This support also requires an appropriate adapter, released separately

“Net::Net” path summary summarizes all enabled application paths during path searches

- QRM now provides the capability to view all enabled ports and protocols across a specific path search
- Network and security engineers can use this capability to easily determine which application paths exist across specified points on the network



Below is a representation of the current network topology model.

Current Filter:

Path from 192.168.240.1/24 to 192.168.230.0/24 and protocol TCP (Clear Filter)

Path Summary:

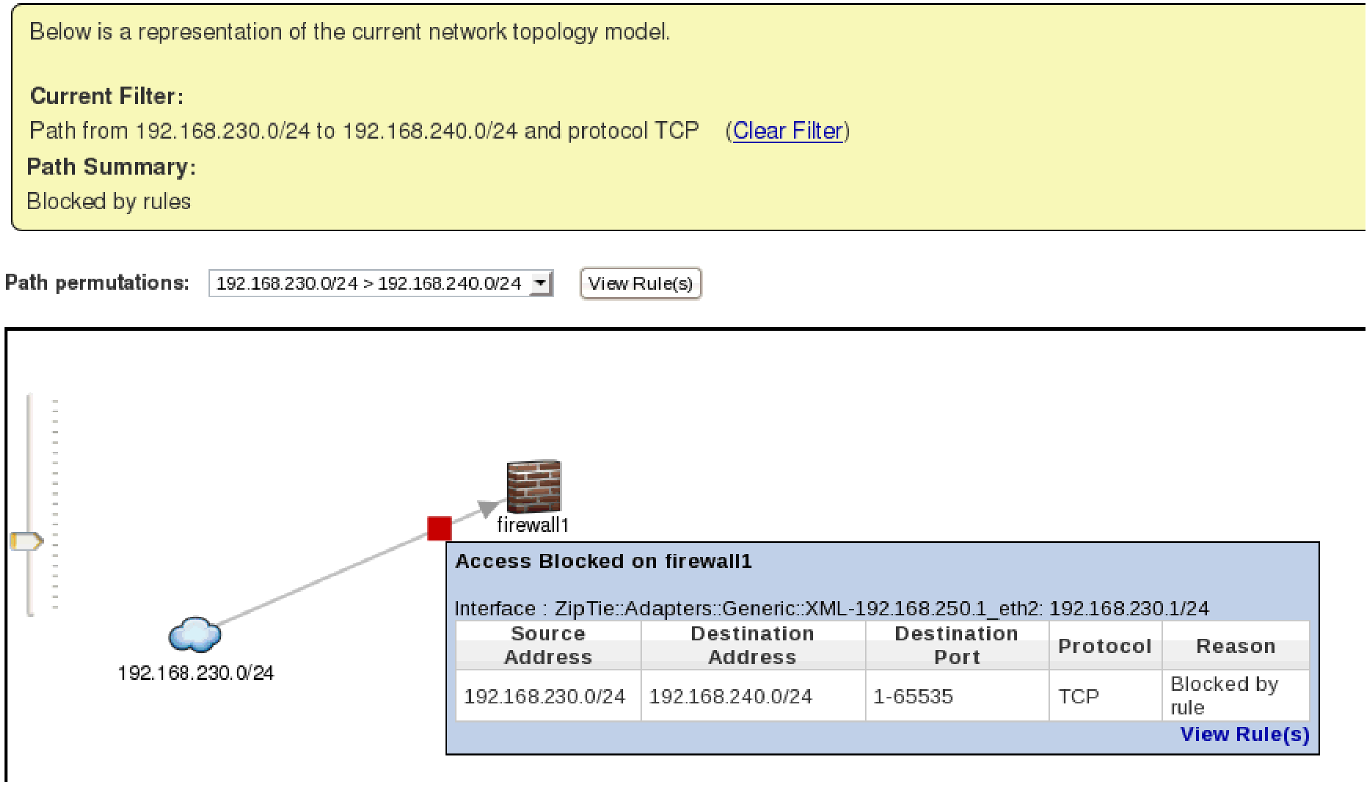
Partially Allowed

Port(s)/Protocol(s): 22 (TCP), 80 (TCP), 443 (TCP)

Path permutations: 192.168.240.0/24 > 192.168.230.0/24

Improved “blocked path” display simplifies analysis of blocked application paths

- Path searches that fail (“no path”) now show the point of the blockage, along with a hover-over option to display the reason
- Users can also display the actual reason for the path blockage (e.g. firewall rules)
- Network and security engineers can use this to quickly determine what changes need to be made in order to enable application paths



Below is a representation of the current network topology model.

Current Filter:

Path from 192.168.230.0/24 to 192.168.240.0/24 and protocol TCP (Clear Filter)

Path Summary:

Blocked by rules

Path permutations: 192.168.230.0/24 > 192.168.240.0/24

Access Blocked on firewall1

Interface : ZipTie::Adapters::Generic::XML-192.168.250.1_eth2: 192.168.230.1/24

Source Address	Destination Address	Destination Port	Protocol	Reason
192.168.230.0/24	192.168.240.0/24	1-65535	TCP	Blocked by rule

View Rule(s)

Major QVM and QRM release

- QRadar Vulnerability Manager
  - Fantastic new capabilities deliver even more value, improve usability and scalability
  - Scan policies reduce scan time, increase performance and flexibility
  - Centralized credentials reduce administration time and overhead
  - Automatic scanner assignment increases scalability, eases administration
  - Asset owner management streamlines en masse owner changes
  - Scheduled scan views enables visualization of scheduled scans, eliminating potential overlaps and improving scan efficiencies
  - PCI ASV, risk prioritized remediation and asset reports and much more!
- QRadar Risk Manager
  - Drastically improved topology performance scales to even larger environments
  - New policy tests enable complex Windows configuration policies like CIS
  - Support for new IPS and Next Gen firewall devices expands topology and policy capabilities
  - Improved path visualizations decrease network administration overhead for users

- Remember to include QVM+QRM in every deal!

ibm.com/security