



# IT Vulnerability Management



# Minimizing Risk by Implementing Vulnerability Management Process

On time – On Budget – On demand

# Agenda

---

- 1. Need for Vulnerability Management
- 2. Vulnerability Management Process
- 3. Capabilities Overview
  - 3.1 Overview
  - 3.2 Software as a Service Model: Security & Coverage
- 4. Summary
  - Advantages & Benefits

# 1. Need for Vulnerability Management

- **Vulnerabilities on a network are GOLD to cyber criminals:**

- Provide unauthorized entry to networks
- Can expose confidential information, fuel stolen identities, violate privacy laws, or paralyse operations
- Exposure is extreme for networks with vulnerable devices connected by IP

## Sources of Vulnerabilities

- ☒ Programming errors
- ☒ Unintentional mistakes or intentional malware in General Public License software
- ☒ Improper system configurations
- ☒ Mobile users sidestepping perimeter security controls
- ☒ Rising attacks through viewing popular websites

# 1. Need for Vulnerability Management

## ■ Despite utilization of basic defenses, network security breaches abound

- TJX exposed 46M records
- DSW exposed 1.4M records
- Card Systems exposed 40M records
- 215M+ reported record exposures since 2005  
(actual is significantly higher)

## ■ Automation is Crucial

- Manual detection and remediation workflow is too slow, too expensive and ineffective

## Attack Trends

- ☒ Increased professionalism and commercialization of malicious activities
- ☒ Threats that are increasingly tailored for specific regions
- ☒ Increasing numbers of multistaged attacks
- ☒ Attackers targeting victims by first exploiting trusted entities
- ☒ Convergence of attack methods
- ☒ Shift from “Hacking for Fame” to “Hacking for Fortune”

# 1. Need for Vulnerability Management

## ■ Did we learn our lessons?

- Most vulnerabilities are long known before exploited
- Successful exploitation of vulnerabilities can cause substantial damage and financial loss
- A few vulnerable systems can disrupt the whole network
- System misconfiguration can make systems vulnerable

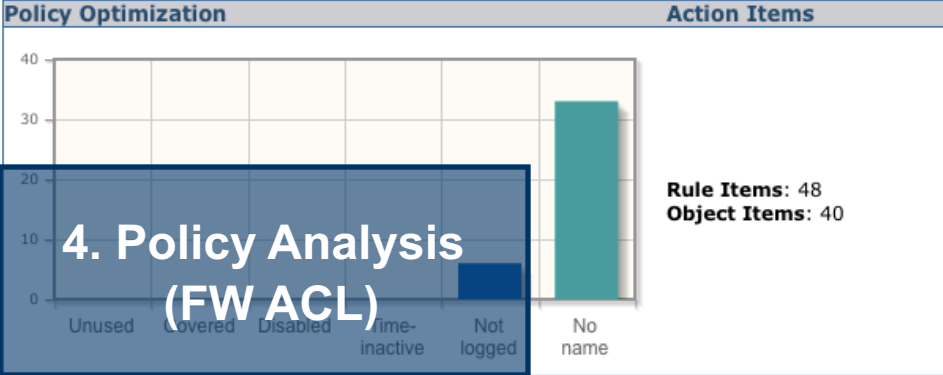
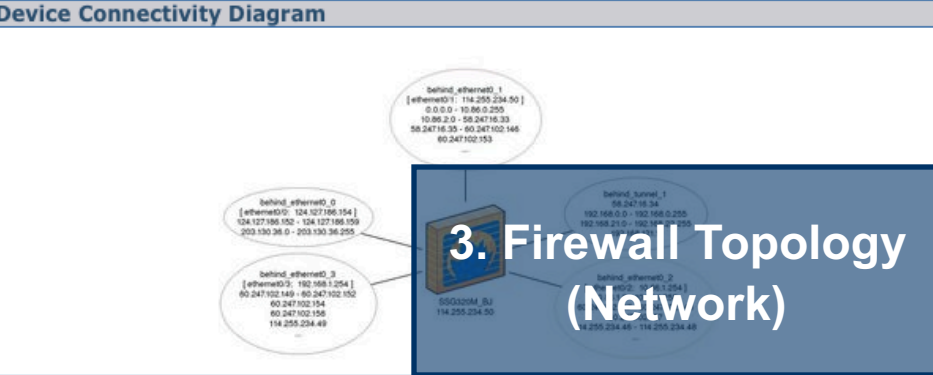
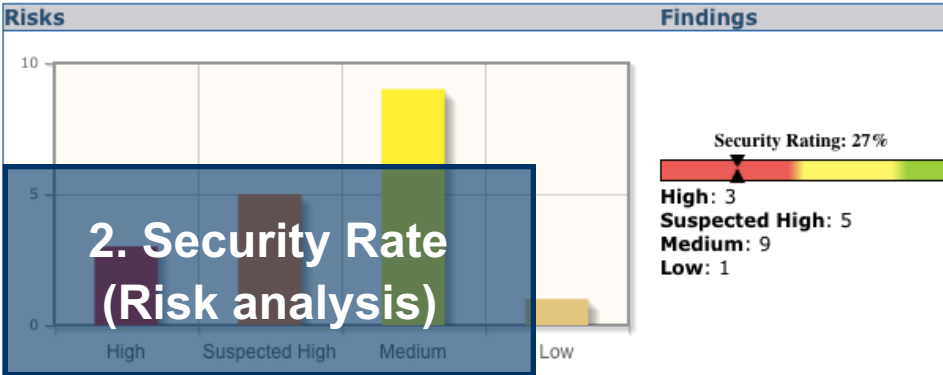
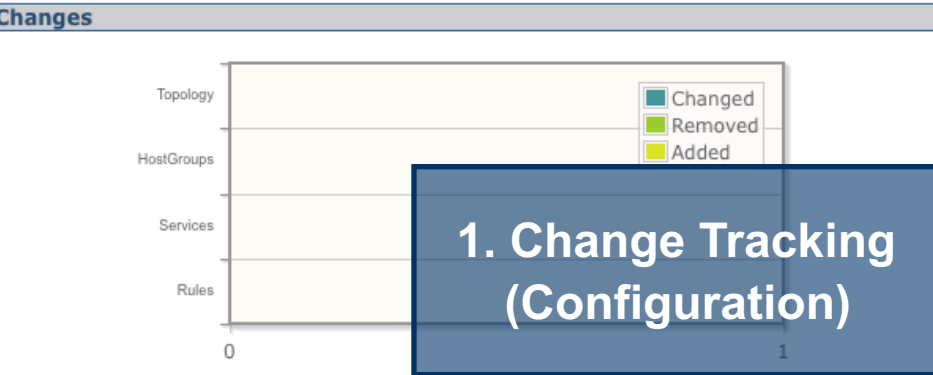
## Challenges IT Security Face

- ☒ NOT enough TIME, PEOPLE, BUDGET
- ☒ Prioritization of efforts for minimize business risks and protecting critical assets. We can't fix all problems - what can we live with?
- ☒ Reduction of operational & capital expenses
- ☒ Adapting to accelerating change in sophistication of attacks and increasing number of regulations

# 1. Firewall Configuration Analysis

## Report example

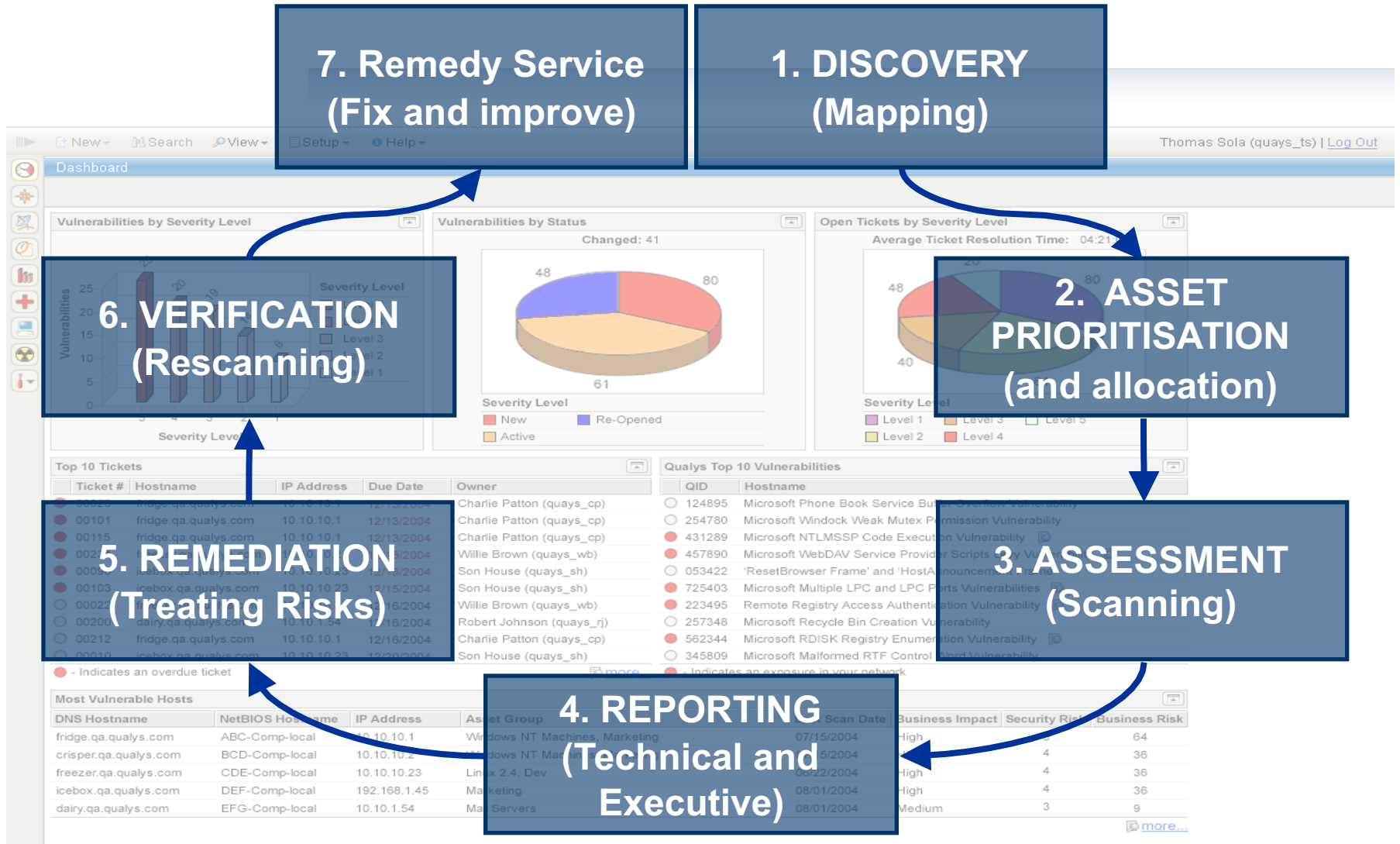
Home: SSG320M\_BJ



### Device Info

Analyzed on: Fri May 10 13:35:23 EDT 2013  
Device Name: SSG320M\_BJ  
IP Address: 114.255.234.50  
Policy: 2013-05-07\_cfg.txt.nsc 38 rules  
Statistics: 239 services and 171 host groups.

# 2. Vulnerability Management Process

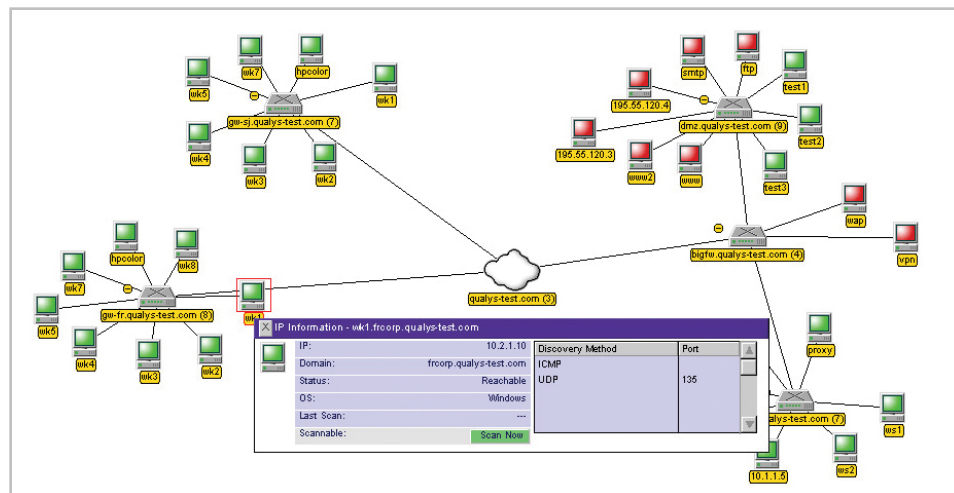




# 2.1 Discovery

## ■ Mapping

- Gives hacker's eye view of you network
- Enables the detection of rogue devices (Shadow IT)



# 2.2 Asset Prioritisation

## ■ Asset Prioritisation

- Some assets are more critical to business than others
- Criticality depends of business impact

## ■ Asset Allocation

- Each asset should have an owner

The screenshot shows a web interface titled "Edit Asset Group". At the top, it states: "An asset group can include IPs, domains/netblocks, and scanner appliances that exist in your account." Below this is the "Asset Group Title" section with two input fields: "Title: \*" containing "SAP Servers" and "Owner: \*" containing "Edvinas Pranculis (Manager: syner-ep)". A navigation bar below contains tabs for "IPs", "Domains", "Users", "Scanner Appliances", and "Business Info", with "Business Info" being the active tab. The "Business Info" section contains four input fields: "Business Impact:" with a dropdown menu set to "Critical" and a "View" link; "Division:" with "Financial Management"; "Function:" with "ERP"; and "Location:" with "Vilnius". Below this is a "Comments:" section with a large empty text area. At the bottom of the form are three buttons: "Save", "Cancel", and "Help".

# 2.3 Assessment

## ■ Signature Classification

- Vulnerability Signatures
- Application Fingerprints
- Service Signatures
- Device / OS Fingerprints
- Configuration Signatures
- Compliance Signatures

## ■ Timely Signatures

- 725+ Devices/OS
- 250+ Remote Services
- 5800+ Vulnerability Signatures
- 950+ Vendors
- 2000+ Products

Vulnerabilities						
View	QID	Category	Title	Severity	CVE ID	
	90332	Windows	Microsoft Windows SMB Malformed PIPE Denial of Service Vulnerability		3	CVE-2006-3942
	115505	Local	Apple QuickDraw GetSrcBits32(ARGB0) Memory Corruption Vulnerability		3	CVE-2007-0462
	115457	Local	Apple Mac OS X FPathConf System Call Local Denial of Service Vulnerability		3	CVE-2006-5836
	1214	Backdoor trojan hor	Storm Worm Detected		4	
	115536	Local	Red Hat mysql Security Update (RHSA-2007-0152)		3	CVE-2006-4226
	43077	Hardware	Cisco VPN 3000 Concentrator Denial of Service Vulnerability		4	
	110057	Office Ap	Microsoft Word 2007 WWLib.DLL Unspecified Document File Buffer Overflow Vulnerability - Zero Day		4	CVE-2007-1910
	110056	Office Ap	Microsoft Publisher 2007 Remote Code Execution Vulnerability - Zero Day		4	CVE-2007-1117
	105294	Security I	Anti-Virus Product Not Detected on the Windows Host		3	
	100040	Internet E	Internet Explorer Denial of Service Vulnerability		3	CVE-2006-5559
	115535	Local	InterActual Player Buffer Overflow in IASystemInfo.dll ActiveX Control		4	CVE-2007-0348
	115534	Local	Red Hat krb5 Security Update (RHSA-2007-0095)		3	CVE-2007-0956, CVE-2007-0957, CVE-2007-1216
	90391	Windows	Windows Kernel Could Allow Elevation of Privilege (MS07-022)		3	CVE-2007-1206
	12236	CGI	Microsoft Content Management Server Could Allow Remote Code Execution (MS07-018)		5	CVE-2007-0938, CVE-2007-0939
	90374	Windows	Vulnerabilities in CSRSS Could Allow Remote Code Execution (MS07-021)		3	CVE-2006-6696, CVE-2007-1209, CVE-2006-6797

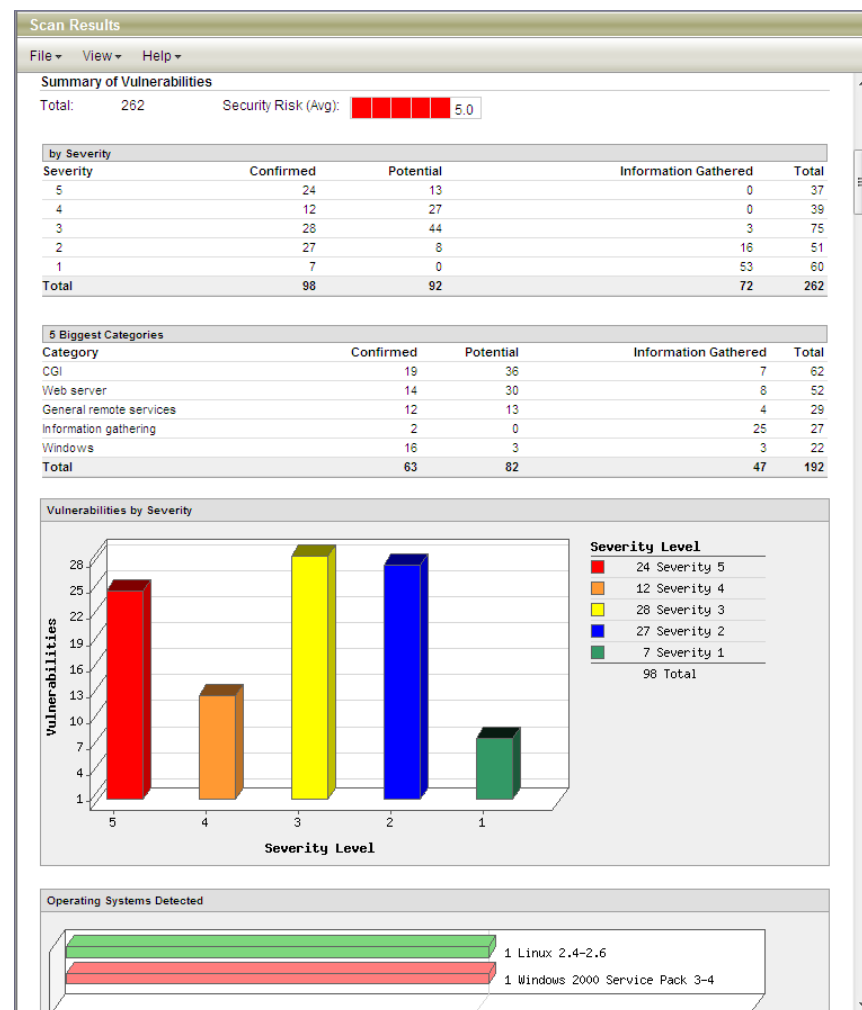
# 2.4 Scanning

## ■ Scanning:

- takes an “outside-in” and “inside-in” approach to security, emulating the attack route of a hacker
- tests effectiveness of security policy and controls by examining network infrastructure for vulnerabilities
- Provides tools for untrusted and authenticated scanning

*“With this product, we gained the ability to automatically scan everything we own for vulnerabilities. And it provides us with a documentation path for all servers including best security practices, vulnerability ranking and patches.”*

Bureau Chief, Strategic IT  
Florida Department of Health



# 2.5 Reporting

## ■ Reporting:

- Allows for generation, storage and distribution of reports for large enterprise networks
- E-mail notifications allow users to review reports upon completion
- Reports can be generated for various compliance initiatives and security requirements:
  - Business Policy, **PCI, SOX, HIPAA, Basel II**, etc.
  - Security trend over a period of time
  - Business risk or CVSS scoring
  - Share reports with auditors, operation staff, security & network managers, executives

Technical Report

File View Help

64.41.134.60 (demo02, DEMO02) Windows 2000 Service Pack 3-4

Vulnerabilities (63)

- 5 Multiple Microsoft Windows Vulnerabilities (MS04-011) New
- 5 Multiple Microsoft Windows RPC/DCOM Vulnerabilities (MS04-012) New

First Detected: 04/08/2008 at 10:48:58 (GMT+0300) Last Detected: 04/08/2008 at 10:48:58 (GMT+0300) Times

Ignore vulnerability Create ticket

QID: 68528  
Category: RPC  
CVE ID: [CVE-2003-0813](#) [CVE-2004-0116](#)  
[CVE-2003-0807](#) [CVE-2004-0124](#)  
Vendor Reference: [MS04-012](#)  
Bugtraq ID: -  
Modified: 10/20/2005  
Edited: No

THREAT:

A security update for multiple vulnerabilities on Microsoft Windows systems is available for download from Microsoft security bulletin [MS04-012](#). The 4 vulnerabilities addressed in the security update include:

- RPC Runtime Library Remote Code Execution Vulnerability - CAN-2003-0813 (Windows 2000, XP, 2003 are affected)
- RPCSS Service Denial Of Service Vulnerability - CAN-2004-0116 (Windows 2000, XP, 2003 are affected)
- COM Internet Services (CIS) RPC over HTTP Denial Of Service Vulnerability - CAN-2003-0807 (Windows NT, 2000, 2003 are affected)
- Object Identity Information Disclosure Vulnerability - CAN-2004-0124 (Windows NT, 2000, XP, 2003 are affected)

IMPACT:

An attacker who successfully exploits the most severe of these vulnerabilities could take complete control of the affected system. An attacker could then take multiple actions on the affected system including installing programs, viewing data, changing data, deleting data, and creating new accounts that have full privileges.

SOLUTION:

Read Microsoft security bulletin [MS04-012](#) for information about this security update and download instructions.

RESULTS:

MS03-026 and MS03-039 patches are not installed.

- 5 Microsoft Messenger Service Buffer Overrun Vulnerability New
- 5 Microsoft SQL Server 2000 Service Pack 4 Missing New
- 5 Microsoft SQL Server Multiple Vulnerabilities New

# 2.5 Reporting



# 2.5 Reporting

■ Reporting:

- Reporting by business units or asset groups
- Security trend over time

*“If you can’t measure security, you can’t manage it. Qualys lets me measure and manage my network security. Their reports demonstrate ongoing security improvement in working with IT suppliers.”*

Director of Global Information Security  
ICI



# 2.6 Remediation

## ■ Remediation

- Tickets are either generated automatically upon scan completion based on policies or on demand by users from any report
- Trouble tickets capture complete audit trails and history of a vulnerabilities on hosts
- QualysGuard scanners verifies the ticket after its closed
- Integration with other helpdesk solutions is available through API

*“In vulnerability management, it’s all about response time. Qualys’ remediation agent directly assigns tickets to fix things to my network technicians. The system then tracks those fixes.”*

Director of Enterprise Security  
**Wescorp**

**Edit Rule**

**Rule Title**

Title: \* Basic Level 4 and 5 Vulnerability Policy for SAP Servers

**Conditions**

If all of the following conditions are met:

**Hosts:**

Asset Groups: SAP Servers [Select](#)

IPs/Ranges: [Select](#)

Example: 192.168.0.87-192.168.0.92, 192.168.0.200

**Vulnerability:**

Severity Levels:

Confirmed Vulnerability:  1  2  3  4  5

Potential Vulnerability:  1  2  3  4  5

Qualys ID:  Select QID numbers that will trigger the creation of a ticket [Configure...](#)

**Actions**

Perform the following actions:

Assign to: Asset Owner [View](#)

Set Deadline: This ticket must be closed in 3 days (Range: 1-120)

Ignore:  Do not create a ticket for these conditions

[Save](#) [Save As...](#) [Cancel](#) [Help](#)



# 2.7 Verification

## ■ Re-scanning:

- Verifies applied patches and confirm compliance
- Verifies the tickets after they are closed

*“Before QG we had an ad hoc process; QG brought much stronger control and visibility into our processes. QG gives us the ability to detect our vulnerabilities across our network and really ensure that we have the level of security and compliance we need.”*

Chief Information Protection Officer  
**CIGNA**

**Critical Asset Verification Report**  
September 20, 2007

Chief Information Security Officer: qualyx\_hd Manager  
Qualys, Inc. 1600 Bridge Parkway RWC, California 94065 United States of America  
Created: 09/20/2007 at 17:23:04 (GMT-0700)

**Summary of Vulnerabilities**  
Total: 453 Security Risk (Avg): 2.1 Business Risk: 17/100

**Vulnerabilities by Status**

Status	Count
Active	235
Re-Opened	7
Fixed	28
New	3

**Detailed Results**  
64.41.134.59 (demo01.qualys.com, DEMO01) Linux 2.4-2.6  
Total: 28 Security Risk: 2.1

Severity	Confirmed	Potential	Information Gathered	Total
5	0	-	-	0
4	0	-	-	0
3	10	-	-	10
2	12	-	-	12
1	6	-	-	6
Total	28	-	-	28

Category	Confirmed	Potential	Information Gathered	Total
General remote services	11	-	-	11
CGI	6	-	-	6
Web server	4	-	-	4
TCPIP	3	-	-	3
Brute Force Attack	2	-	-	2
Total	26	-	-	26

**Vulnerabilities (28)**

- Discovery of Unix Account Names Vulnerability port:80/ftp CVSS: 6.5 Active
- Webalizer Web Usage Statistics Accessible port:80/ftp CVSS: 6 Active

# 2.8 Remedy Service

## ■ Before & After

- Network Facilities
- Host Servers
- Firewall Policies
- Virtualization Environment

before	Windows 2008 R2 / Windows 7	after	Windows 2008 R2 / Windows 7
	Severity Vulnerabilities (3)		Severity Vulnerabilities (10)
	5 0		5 0
	4 0		4 0
	3 3		3 3
	2 0		2 5
	1 0		1 2
	Potential Vulnerabilities (1)		Potential Vulnerabilities (3)
	Severity		Severity
	5 0		5 0
	4 0		4 0
	3 1		3 1
	2 0		2 2
	1 0		1 0

before	Polycom HDX 7000	after	Polycom HDX 7000
	Severity Vulnerabilities (4)	hosts not scanned, host not alive	
	5 1		
	4 0		
	3 3		
	2 0		
	1 0		
	Potential Vulnerabilities (1)		
	Severity		
	5 1		
	4 0		
	3 0		
	2 0		
	1 0		

before	Polycom HDX 7000	after	Polycom HDX 7000
	Severity Vulnerabilities (5)	hosts not scanned, host not alive	
	5 1		
	4 0		
	3 4		
	2 0		
	1 0		
	Potential Vulnerabilities (1)		
	Severity		
	5 1		
	4 0		
	3 0		
	2 0		
	1 0		

before	Windows 2003	after	Windows 2003
	Severity Vulnerabilities (5)		Severity Vulnerabilities (6)
	5 0		5 0
	4 0		4 0
	3 5		3 4
	2 0		2 2
	1 0		1 0
	Potential Vulnerabilities (0)		Potential Vulnerabilities (2)
	Severity		Severity
	5 0		5 0
	4 0		4 0
	3 0		3 1
	2 0		2 1
	1 0		1 0

before	Polycom HDX 7000	after	Polycom HDX 7000
	Severity Vulnerabilities (2)		Severity Vulnerabilities (1)
	5 0		5 0
	4 0		4 0
	3 2		3 0
	2 0		2 1
	1 0		1 0
	Potential Vulnerabilities (0)		Potential Vulnerabilities (2)
	Severity		Severity
	5 0		5 0
	4 0		4 0
	3 0		3 0
	2 0		2 0
	1 0		1 0

before	Polycom HDX 7000	after	Polycom HDX 7000
	Severity Vulnerabilities (6)		Severity Vulnerabilities (6)
	5 0		5 0
	4 0		4 0
	3 2		3 2
	2 4		2 4
	1 0		1 0
	Potential Vulnerabilities (0)		Potential Vulnerabilities (2)
	Severity		Severity
	5 0		5 0
	4 0		4 0
	3 0		3 1
	2 0		2 1
	1 0		1 0

# 3. Benefits of Vulnerability Management

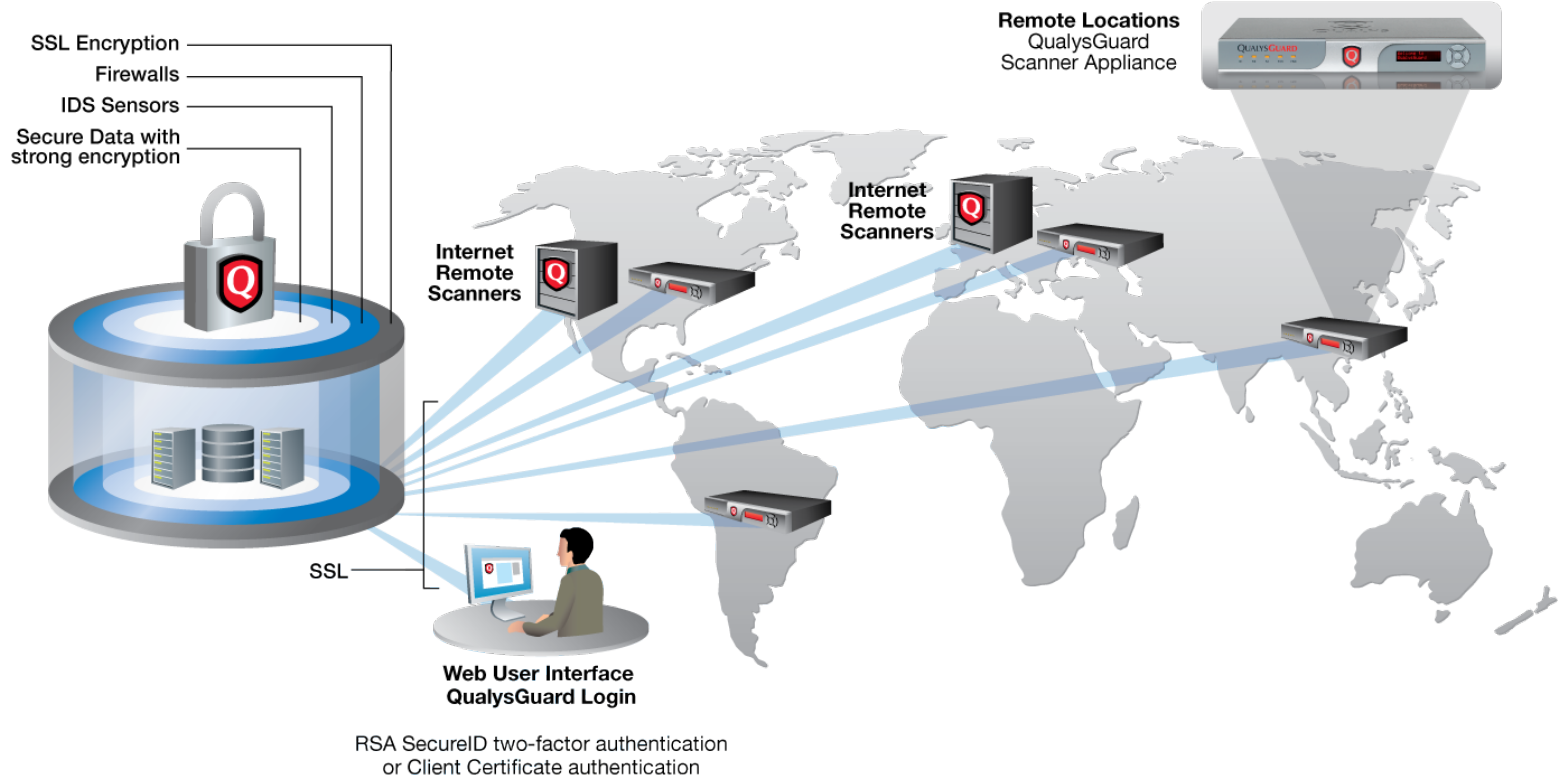
- Vulnerability management gives you control and visibility to manage your networks security effectively and document compliance
- Vulnerability management is PROACTIVE approach to security

*“Enterprises that implement a **vulnerability management** process will experience **90% fewer successful attacks** than those that make an equal investment only in intrusion detection systems.”*

**Gartner**

# 3.1 QualysGuard (SaaS mode)

## QualysGuard Secure Operations Centers (SOCs)



- Deployability** ■ 6 000+ Appliances Deployed in >65 Countries
- Largest Single Enterprise Deployment: 223 Appliances in 52 Countries
- Scalability** ■ 200+ Million IP Audits Per Year
- Reliability** ■ Six Sigma (99.99966%) Accuracy: <3.4 Defects per 1 Million Scans

# 3.2 Case Study by Industries

### Insurance

### Financial Services

### Financial Services

### Chemical

### Portals/Internet

### Retail

### Technology

### Consulting

# 3.2 Case Study by Industries

## Media



## Energy/Utilities



## Consumer Products



## Health Care



## Manufacturing



## Education



## Transportation



## Government



# 4. Summary

---

## ■ The Benefits of BROTIGHT Vulnerability Management Service & QualysGuard Platform:

- Gives you control and visibility to manage your networks security risks effectively and document compliance
- Automates most elements of Vulnerability Management in an efficient, cost-effective manner
- Enables you to cut your vulnerability management expenses by 50-90% when compared to traditional enterprise-software VM solutions
- With BROTIGHT professional service, you could reduce the risk of IT infrastructure via periodicity site/cloud service and keep your infrastructure running on manageable risk control.



**谢谢!**

**THANKS FOR THE BUSINESS**