QUALYS®

WHITE PAPER

7 ESSENTIAL STEPS TO ACHIEVE, MEASURE AND PROVE OPTIMAL SECURITY RISK REDUCTION

Table of Contents

ON DEMAND SECURITY

I. Overview

Risks that threaten the security and availability of networks and applications range from newfound software and operating system vulnerabilities—announced at a rate of 155 a week in 2006—to misconfigurations and errors that easily creep into server, firewall, and end-point settings. Rapid changes within technology, new server and software deployments, and the evolving sophistication of attack methods used to infiltrate systems and steal data create the greatest set of challenges faced by security and IT administrators trying to keep their systems secure and within regulatory compliance.

That's why—whether protecting five servers or 5,000—measuring the security status of your infrastructure and your organization's ability to rapidly mitigate emerging threats needs to be continuously monitored and measured.

It's impossible to secure what isn't measured. Without an accurate depiction of your network, the ability to identify real-world security threats and evaluate your organization's ability to respond, there's no way to improve, let alone understand, the true security posture of your infrastructure. More and more, companies seeking to better manage complex threats and increased regulatory demands are enhancing their security efforts by establishing effective and sustainable vulnerability and risk management programs that quantify their security progress to maintain the confidentiality, integrity, and availability of business data and networks.

> *"You can't manage what you can't measure."*
>
> Peter Drucker
> **Management Visionary & Author**

II. Risk Reduction and Continuous Security Improvement: Measuring What Matters

Measuring the effectiveness of your IT security and vulnerability management program doesn't mean increased workload for security managers and system administrators. In fact, with the right tools in place, collecting, correlating, and analyzing IT security information should be integrated into the workflow already in place to identify and fix your unpatched and misconfigured systems.

The goal is to track the progress of your vulnerability management program in ways that give administrators the information they need to swiftly remedy at-risk systems, while also providing business leaders the insight they need to understand their company's overall levels of risk. This is accomplished by obtaining an accurate network baseline, classifying IT systems, identifying and prioritizing system vulnerabilities, validating their remediation, and capturing the intelligence needed to measure security posture and improvement over time.

> *The goal of your vulnerability management program is to give administrators the information needed to quickly remediate issues, while providing business leaders the insight they need to understand the company's overall risk.*

QualysGuard, from Qualys Inc., is the leading on-demand security risk and compliance management solution. QualysGuard enables businesses of all sizes to strengthen the security of their networks through automated security audits that capture everything they need to quantify and measure their security posture, including the ability to: Discover and prioritize all network assets; proactively identify and fix security vulnerabilities; manage and reduce business risk; and ensure steady compliance with IT security laws, industry regulations, and internal security policies.

Delivered as an on-demand Web-based service, QualysGuard requires no hardware or software to install or maintain, is deployable in hours, and provides an immediate view of security and regulatory compliance readiness. With more than 150 million IP audits conducted annually, QualysGuard is the most widely deployed on-demand security solution in the world.

This paper details the essential aspects of a putting into place a measurable and sustainable vulnerability management program, and demonstrates how QualysGuard automates everything you need along the way.

ESSENTIAL STEP 1: Discover Baseline Network Assets

The first step is to establish an accurate baseline and map of your network. In this stage, each network asset needs to be identified: servers, desktops, notebooks, routers, wireless access points, networked printers, and other connected devices. This baseline provides the foundation for managing and measuring your vulnerability management program. Your network baseline will continuously change as new servers, applications, and devices are deployed. That's why it's vital to have the ability to update the status of your network as often as needed.

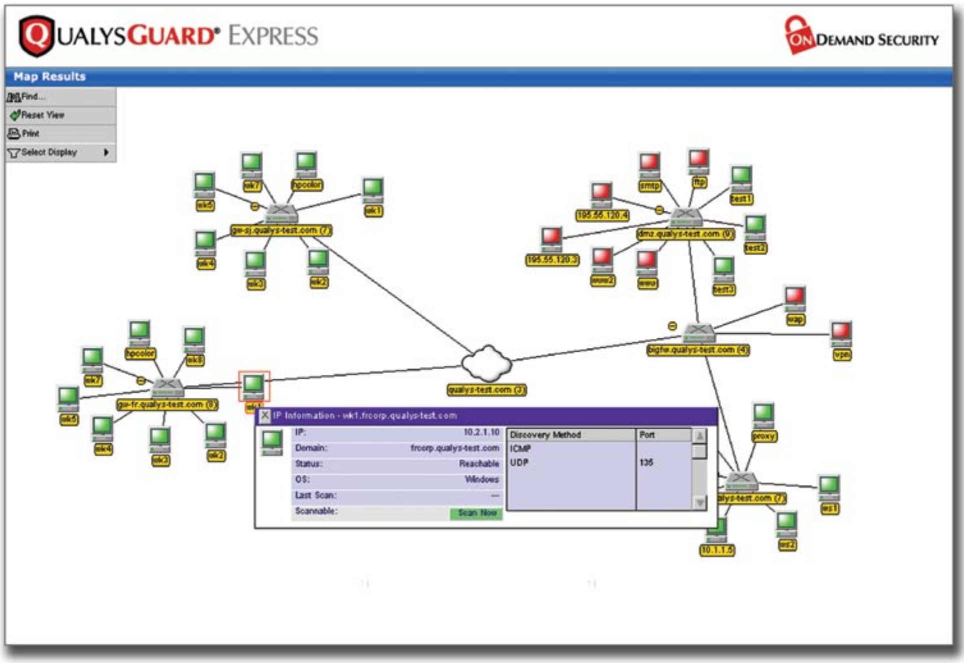
How QualysGuard Automates Network Discovery and Mapping

QualysGuard rapidly detects and identifies all of your networked IT assets—servers, desktops, routers, and other networked devices. QualysGuard makes no assumptions about any aspects of the infrastructure, and identifies all assets and vulnerabilities on all 65,536 ports. The result is a powerful and highly accurate baseline of your network that includes each connected device. The QualysGuard network map can be viewed as a visual representation or as a standard report.

The QualysGuard network map can be used to classify the business value of each device, and to obtain trend information on how well security efforts are improving over time. This powerful representation of your network also can be used to initiate on-demand or pre-scheduled scans to examine the security of each asset or area of your network.

QualysGuard discovers and depicts your entire network topology:

- *All network access points.*
- *The hostname of every system.*
- *Both static and dynamic IP addresses.*
- *Every operating system.*
- *Common communication services, including HTTP, SMTP, Telnet, and others.*



IP Information - wk1.frcorp.qualys-test.com

IP: 10.2.1.10
Domain: frcorp.qualys-test.com
Status: Reachable
OS: Windows
Last Scan: ---
Scannable:

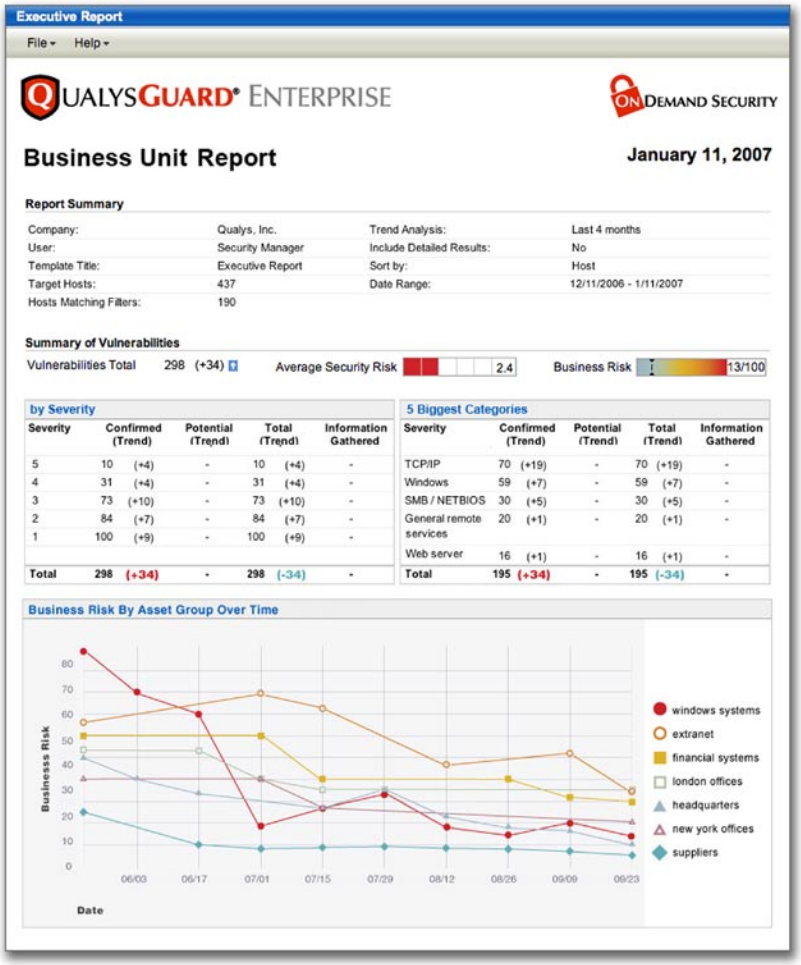
Discovery Method	Port
ICMP	
UDP	135

Figure 1: QualysGuard Discovery Map

ESSENTIAL STEP 2: Asset Classification

Following full network discovery, the next phase is to classify the business value of your desktops, servers, and applications. It's essential that networked devices be grouped and classified from what are low-priority systems, such as segmented test systems, to medium-priority systems like the notebooks used by your sales team, to the most critical systems that govern regulated information or are vital to business operations and cash flow. How you classify your systems depends on the nature of your business. For example, while Web servers and systems that support order fulfillment, including those regulated by PCI DSS, may be the most critical devices for an Internet merchant, it could be all of the systems that support the supply chain for a manufacturer. The goal is to identify those systems that are essential to business operations and success. Additionally, all systems that handle regulated—or private customer—information need to be classified accordingly.

By classifying IT assets, you'll be able to respond in the most effective way possible, and mitigate those risks that target your most crucial assets and business units.



Business Unit Report January 11, 2007

Report Summary

Company:	Qualys, Inc.	Trend Analysis:	Last 4 months
User:	Security Manager	Include Detailed Results:	No
Template Title:	Executive Report	Sort by:	Host
Target Hosts:	437	Date Range:	12/11/2006 - 1/11/2007
Hosts Matching Filters:	190		

Summary of Vulnerabilities

Vulnerabilities Total 298 (+34) Average Security Risk 2.4 Business Risk 13/100

by Severity

Severity	Confirmed (Trend)	Potential (Trend)	Total (Trend)	Information Gathered
5	10 (+4)	-	10 (+4)	-
4	31 (+4)	-	31 (+4)	-
3	73 (+10)	-	73 (+10)	-
2	84 (+7)	-	84 (+7)	-
1	100 (+9)	-	100 (+9)	-
Total	298 (+34)	-	298 (-34)	-

5 Biggest Categories

Severity	Confirmed (Trend)	Potential (Trend)	Total (Trend)	Information Gathered
TCP/IP	70 (+19)	-	70 (+19)	-
Windows	59 (+7)	-	59 (+7)	-
SMB / NETBIOS	30 (+5)	-	30 (+5)	-
General remote services	20 (+1)	-	20 (+1)	-
Web server	16 (+1)	-	16 (+1)	-
Total	195 (+34)	-	195 (-34)	-

Business Risk By Asset Group Over Time

Figure 2: QualysGuard Business Unit Reports enable detailed asset classification and business unit grouping.

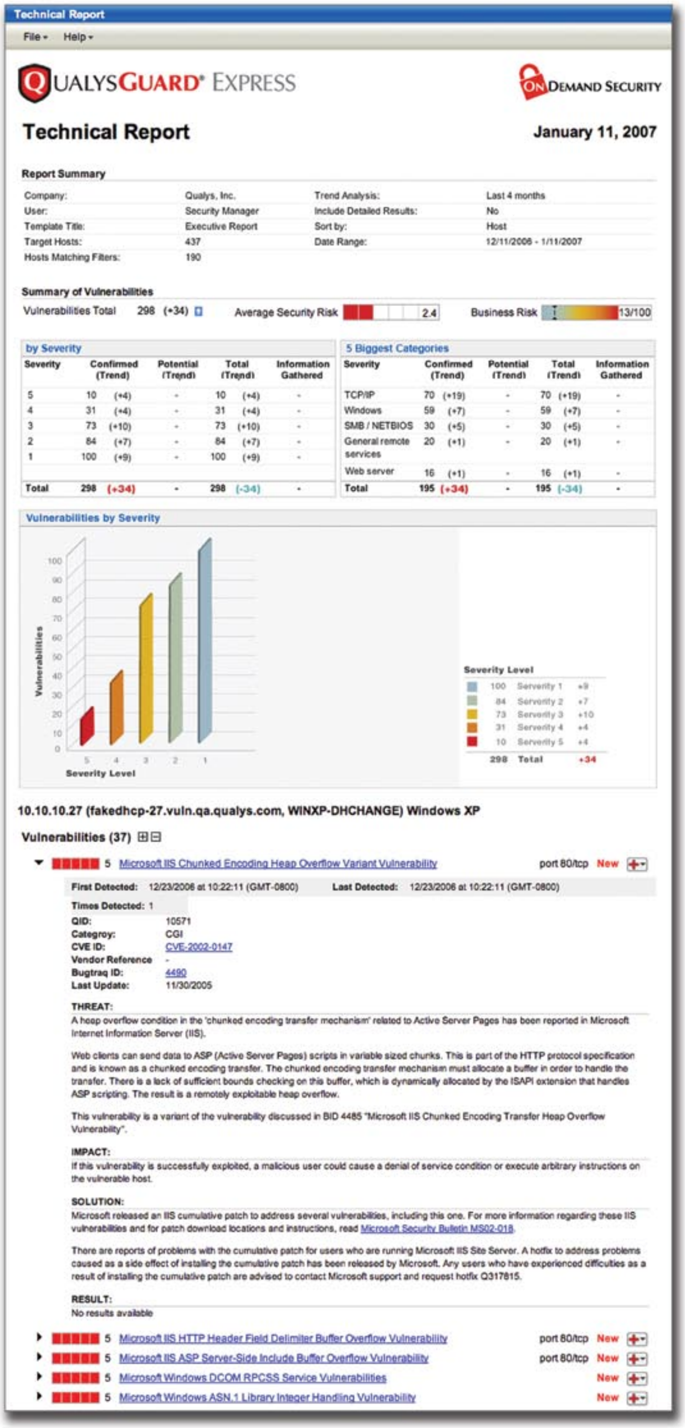
How QualysGuard Streamlines Asset Classification

QualysGuard makes it possible for you to centrally manage all network assets, and quickly identify those that are out of policy, misconfigured, or otherwise vulnerable. Even hosts that are automatically assigned dynamic addresses can be identified easily and tracked through QualysGuard's Dynamic Host Management (DHCP) capabilities. QualysGuard enables assets to be custom tagged for enhanced classification levels. QualysGuard asset tags can be customized for each scan, and provide a powerful way to tag, track and manage every networked device. And QualysGuard provides additional asset qualification levels, allowing customers to group assets into specific business units in any way desired.

ESSENTIAL STEP 3: Swift, Accurate Vulnerability Identification

Modern networks are complex, with most organizations supporting various server, operating system and Web platforms. What's needed is a highly accurate, comprehensive, and up-to-date way to identify the latest system vulnerabilities and misconfigurations based on timely information and your precise system and network configurations. Proper "Defense in Depth" security requires that the strongest possible vulnerability detection and management system is implemented. This ensures that the vulnerabilities identified pose real-world risks to your organization, and that administrators don't waste time chasing vulnerabilities that don't actually exist (false positives).

Too many organizations will run a vulnerability assessment and blindly begin patching the most critical vulnerabilities first, then move toward their medium and low risks. While this is certainly one way to approach the problem, it's not always the most effective route to risk reduction. The fact is that critical vulnerabilities on certain systems often can be a lower priority than medium vulnerabilities on your most important systems. That's why it's important to correlate vulnerability criticality (typically in levels ranging from 1 to 5) with the business value of vulnerability systems and network segments. You want to mitigate the most vital, and regulated systems first.



Technical Report

January 11, 2007

Report Summary

Company:	Qualys, Inc.	Trend Analysis:	Last 4 months
User:	Security Manager	Include Detailed Results:	No
Template Title:	Executive Report	Sort by:	Host
Target Hosts:	437	Date Range:	12/11/2006 - 1/11/2007
Hosts Matching Filters:	190		

Summary of Vulnerabilities

Vulnerabilities Total 298 (+34) Average Security Risk 2.4 Business Risk 13/100

by Severity

Severity	Confirmed (Trend)	Potential (Trend)	Total (Trend)	Information Gathered
5	10 (+4)	-	10 (+4)	-
4	31 (+4)	-	31 (+4)	-
3	73 (+10)	-	73 (+10)	-
2	84 (+7)	-	84 (+7)	-
1	100 (+9)	-	100 (+9)	-
Total	298 (+34)	-	298 (-34)	-

5 Biggest Categories

Severity	Confirmed (Trend)	Potential (Trend)	Total (Trend)	Information Gathered
TCP/IP	70 (+19)	-	70 (+19)	-
Windows	59 (+7)	-	59 (+7)	-
SMB / NETBIOS	30 (+5)	-	30 (+5)	-
General remote services	20 (+1)	-	20 (+1)	-
Web server	16 (+1)	-	16 (+1)	-
Total	195 (+34)	-	195 (-34)	-

Vulnerabilities by Severity

Severity Level

🟦	100	Serverity 1	+9
🟩	84	Serverity 2	+7
🟨	73	Serverity 3	+10
🟧	31	Serverity 4	+4
🟥	10	Serverity 5	+4
	298	Total	+34

10.10.10.27 (fakedhcp-27.vuln.qa.qualys.com, WINXP-DHCHANGE) Windows XP

Vulnerabilities (37)

▾ 5 Microsoft IIS Chunked Encoding Heap Overflow Variant Vulnerability port 80/tcp New

First Detected: 12/23/2006 at 10:22:11 (GMT-0800) Last Detected: 12/23/2006 at 10:22:11 (GMT-0800)

Times Detected: 1

QID:	10571
Categroy:	CGI
CVE ID:	CVE-2002-0147
Vendor Reference	-
Bugtraq ID:	4490
Last Update:	11/30/2005

THREAT:

A heap overflow condition in the 'chunked encoding transfer mechanism' related to Active Server Pages has been reported in Microsoft Internet Information Server (IIS).

Web clients can send data to ASP (Active Server Pages) scripts in variable sized chunks. This is part of the HTTP protocol specification and is known as a chunked encoding transfer. The chunked encoding transfer mechanism must allocate a buffer in order to handle the transfer. There is a lack of sufficient bounds checking on this buffer, which is dynamically allocated by the ISAPI extension that handles ASP scripting. The result is a remotely exploitable heap overflow.

This vulnerability is a variant of the vulnerability discussed in BID 4485 "Microsoft IIS Chunked Encoding Transfer Heap Overflow Vulnerability".

IMPACT:

If this vulnerability is successfully exploited, a malicious user could cause a denial of service condition or execute arbitrary instructions on the vulnerable host.

SOLUTION:

Microsoft released an IIS cumulative patch to address several vulnerabilities, including this one. For more information regarding these IIS vulnerabilities and for patch download locations and instructions, read Microsoft Security Bulletin MS02-018.

There are reports of problems with the cumulative patch for users who are running Microsoft IIS Site Server. A hotfix to address problems caused as a side effect of installing the cumulative patch has been released by Microsoft. Any users who have experienced difficulties as a result of installing the cumulative patch are advised to contact Microsoft support and request hotfix Q317815.

RESULT:

No results available

▸ 5 Microsoft IIS HTTP Header Field Delimiter Buffer Overflow Vulnerability port 80/tcp New

▸ 5 Microsoft IIS ASP Server-Side Include Buffer Overflow Vulnerability port 80/tcp New

▸ 5 Microsoft Windows DCOM RPCSS Service Vulnerabilities New

▸ 5 Microsoft Windows ASN.1 Library Integer Handling Vulnerability New

Figure 3: QualysGuard Technical Report helps administrators effectively pinpoint and fix critical issues fast.

How QualysGuard Automates Accurate Vulnerability Analysis

QualysGuard's on-demand vulnerability assessments examine your infrastructure against the most accurate, up-to-date vulnerability database in the industry. The QualysGuard solution includes its own KnowledgeBase of vulnerability signatures which is updated daily to deliver Six Sigma accuracy (99.997%) via painstaking testing of each signature. The result is unmatched scanning breadth and accuracy for every audit.

QualysGuard's powerful classification and categorization of vulnerabilities enables the creation of specific metrics for various types of vulnerabilities. This configuration-based vulnerability reporting capability provides metrics relevant for measuring organizational security awareness, program effectiveness and adherence to corporate security policies.

By prioritizing remediation efforts based on IT asset values and vulnerability criticality, you're first reducing the risks that pose the greatest threat to your organization.

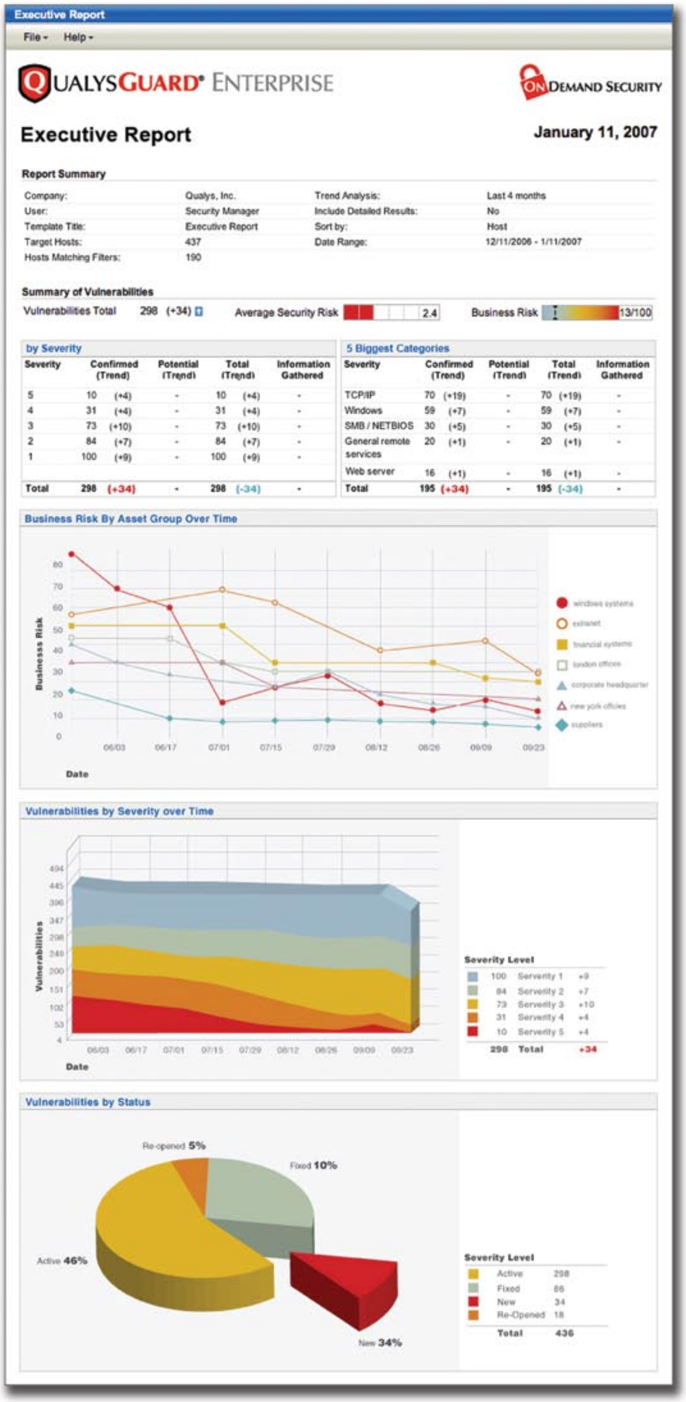
ESSENTIAL STEP 4: Transform Raw Security Data into Intelligence through Comprehensive Reporting

Reading listings of unrefined vulnerabilities is of little value when measuring security levels. What administrators need are comprehensive reports that detail vulnerability criticality and provide instant access to verified remediation solutions, whether they be software vendor patches, workarounds, or other defensive strategies.

In addition to generating reports geared toward system administrators and security managers, security information needs to be collected, customized, and presented to others who need information regarding the security status of your organization. These include demonstrating high levels of security and regulatory compliance to management, regulators, acquiring banks (in the case of PCI DSS), and even to business partners and customers who may request information regarding your IT security efforts.

How QualysGuard Automates IT Security Reporting and Auditing

QualysGuard automatically generates comprehensive, yet easy-to-understand, vulnerability reports that quantify system risks and provide administrators with all of the information they need for fast and effective remediation, even by individual business units. Vulnerabilities are ranked by criticality through the 1-through-5 industry standard, including vulnerability links to Bugtraq and the Common Vulnerabilities and Exposures (CVE) dictionary maintained by Mitre Corp. QualysGuard's predefined reports also highlight your organization's level of protection against the SANS Top 20 listing of the most critical vulnerabilities, as well as insight into the ten most prevalent vulnerabilities in your internal and externally-facing infrastructure. QualysGuard gives organizations the ability to mitigate their most pressing vulnerabilities in the fastest way possible.



Executive Report

January 11, 2007

Report Summary

Company:	Qualys, Inc.	Trend Analysis:	Last 4 months
User:	Security Manager	Include Detailed Results:	No
Template Title:	Executive Report	Sort by:	Host
Target Hosts:	437	Date Range:	12/11/2006 - 1/11/2007
Hosts Matching Filters:	190		

Summary of Vulnerabilities

Vulnerabilities Total 298 (+34) Average Security Risk 2.4 Business Risk 13/100

by Severity

Severity	Confirmed (Trend)	Potential (Trend)	Total (Trend)	Information Gathered
5	10 (+4)	-	10 (+4)	-
4	31 (+4)	-	31 (+4)	-
3	73 (+10)	-	73 (+10)	-
2	84 (+7)	-	84 (+7)	-
1	100 (+9)	-	100 (+9)	-
Total	298 (+34)	-	298 (-34)	-

5 Biggest Categories

Severity	Confirmed (Trend)	Potential (Trend)	Total (Trend)	Information Gathered
TCP/IP	70 (+19)	-	70 (+19)	-
Windows	59 (+7)	-	59 (+7)	-
SMB / NETBIOS	30 (+5)	-	30 (+5)	-
General remote services	20 (+1)	-	20 (+1)	-
Web server	16 (+1)	-	16 (+1)	-
Total	195 (+34)	-	195 (-34)	-

Business Risk By Asset Group Over Time

Vulnerabilities by Severity over Time

Severity Level

■	100	Serverity 1	+9
■	84	Serverity 2	+7
■	73	Serverity 3	+10
■	31	Serverity 4	+4
■	10	Serverity 5	+4
	298	Total	+34

Vulnerabilities by Status

Severity Level

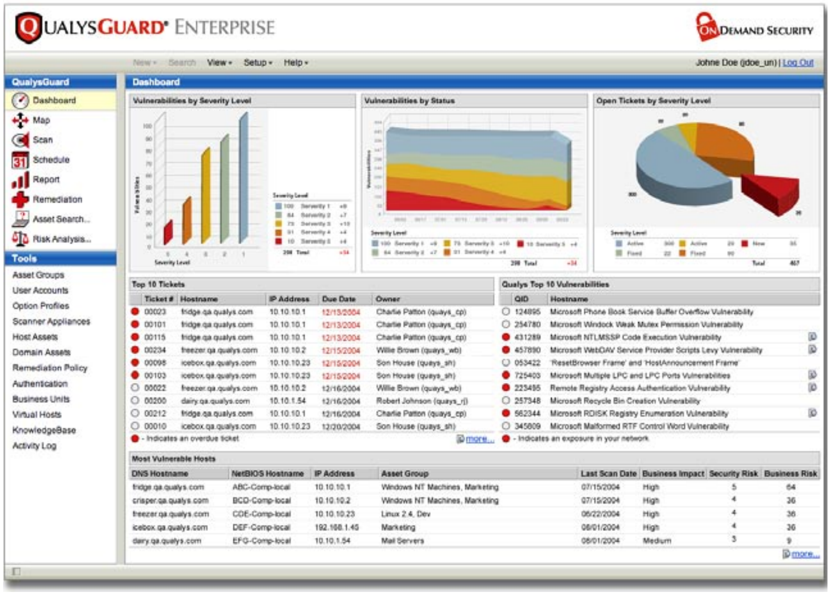
■	Active	298
■	Fixed	86
■	New	34
■	Re-Opened	18
	Total	436

Figure 4: QualysGuard Executive Reports provide senior management with an accurate understanding of the organizations security posture

ESSENTIAL STEP 5: Dynamic Dashboards & The Ability to Measure and Trend Security Posture over Time

Dashboards create instant, near real-time insight into the risk posture of your organization by visually representing overall network health. The Dashboard needs to be kept continuously up-to-date and customizable for your specific business and security needs.

With each vulnerability assessment, a record is created that tracks the date and time of the scan, the number of identified vulnerabilities, their severity, and the business value, or classification, of each system. Once patches have been deployed, a subsequent scan validates that each system patch had been properly applied and its associated risks mitigated. The ability to track how long it takes your organization to identify, remedy, and validate patch deployments is fundamental. This measurement highlights how well your vulnerability management program is working; thus, by reducing the number of days it takes to patch vulnerable systems, administrators can demonstrate to business managers how they're reducing organizational risk.



Top 10 Tickets

	Ticket #	Hostname	IP Address	Due Date	Owner
●	00023	fridge.qa.qualys.com	10.10.10.1	12/13/2004	Charlie Patton (quays_cp)
●	00101	fridge.qa.qualys.com	10.10.10.1	12/13/2004	Charlie Patton (quays_cp)
●	00115	fridge.qa.qualys.com	10.10.10.1	12/13/2004	Charlie Patton (quays_cp)
●	00234	freezer.qa.qualys.com	10.10.10.2	12/15/2004	Willie Brown (quays_wb)
●	00098	icebox.qa.qualys.com	10.10.10.23	12/15/2004	Son House (quays_sh)
●	00103	icebox.qa.qualys.com	10.10.10.23	12/15/2004	Son House (quays_sh)
○	00022	freezer.qa.qualys.com	10.10.10.2	12/16/2004	Willie Brown (quays_wb)
○	00200	dairy.qa.qualys.com	10.10.1.54	12/16/2004	Robert Johnson (quays_rj)
○	00212	fridge.qa.qualys.com	10.10.10.1	12/16/2004	Charlie Patton (quays_cp)
○	00010	icebox.qa.qualys.com	10.10.10.23	12/20/2004	Son House (quays_sh)

● - Indicates an overdue ticket more...

Qualys Top 10 Vulnerabilities

	QID	Hostname
○	124895	Microsoft Phone Book Service Buffer Overflow Vulnerability
○	254780	Microsoft Windock Weak Mutex Permission Vulnerability
●	431289	Microsoft NTLMSSP Code Execution Vulnerability
●	457890	Microsoft WebDAV Service Provider Scripts Levy Vulnerability
○	053422	'ResetBrowser Frame' and 'HostAnnouncement Frame'
●	725403	Microsoft Multiple LPC and LPC Ports Vulnerabilities
●	223495	Remote Registry Access Authentication Vulnerability
○	257348	Microsoft Recycle Bin Creation Vulnerability
●	562344	Microsoft RDISK Registry Enumeration Vulnerability
○	345809	Microsoft Malformed RTF Control Word Vulnerability

● - Indicates an exposure in your network

Most Vulnerable Hosts

DNS Hostname	NetBIOS Hostname	IP Address	Asset Group	Last Scan Date	Business Impact	Security Risk	Business Risk
fridge.qa.qualys.com	ABC-Comp-local	10.10.10.1	Windows NT Machines, Marketing	07/15/2004	High	5	64
crisper.qa.qualys.com	BCD-Comp-local	10.10.10.2	Windows NT Machines, Marketing	07/15/2004	High	4	36
freezer.qa.qualys.com	CDE-Comp-local	10.10.10.23	Linux 2.4, Dev	06/22/2004	High	4	36
icebox.qa.qualys.com	DEF-Comp-local	192.168.1.45	Marketing	08/01/2004	High	4	36
dairy.qa.qualys.com	EFG-Comp-local	10.10.1.54	Mail Servers	08/01/2004	Medium	3	9

more...

Figure 5: QualysGuard Executive Dashboard provides a holistic view of risks and the progress being made to ensure network security.

Also, areas of weakness can be identified, such as servers consistently maintained below policy, or that certain business groups or IT administrators are taking too much time to remedy at-risk systems. By trending the time-to-patch, and correlating that information with the business value of your IT assets, you also can track your organization's overall success at keeping systems in line with your internal security policies—such as patching all critical systems within one week of identifying a vulnerability, and within two weeks for others. Other key metrics worth tracking include the degree at which all end-points and servers are maintained within regulatory compliance, how many systems remain vulnerable over time, and the percentage of systems consistently maintained within your IT security policy.

How QualysGuard Automates the Executive Dashboard to Enable Deep Insight

The QualysGuard Executive Dashboard provides an interactive portal that illustrates your risk level in near real-time. QualysGuard Dashboards can be customized to display vulnerability and remediation information, and overall security posture for administrators and business managers alike. This interactive portal visually highlights your greatest security risks and most urgent remediation tickets in real-time. All aspects of your vulnerability management status are displayed, including vulnerability trends, open remediation tickets, and tailored Top 10 vulnerability lists and rankings of your most vulnerable systems.

QualysGuard delivers the technical insight that security managers need for effective remediation and the high-level risk summaries business managers need to understand. QualysGuard trending reports can be generated through dozens of predefined formats, or highly-customized for your organization. QualysGuard summarizes the security status of each network device, including scan information, specific host information, and a listing of detected vulnerabilities. Based on scanning histories, QualysGuard automatically provides trend analysis and differential reports that detail your security policy compliance. Managers and executives can easily use this information to allocate security budgets, update insurers, and demonstrate your security due-diligence efforts to business partners, regulators, and customers.

ESSENTIAL STEP 6: Remediation Process Integration

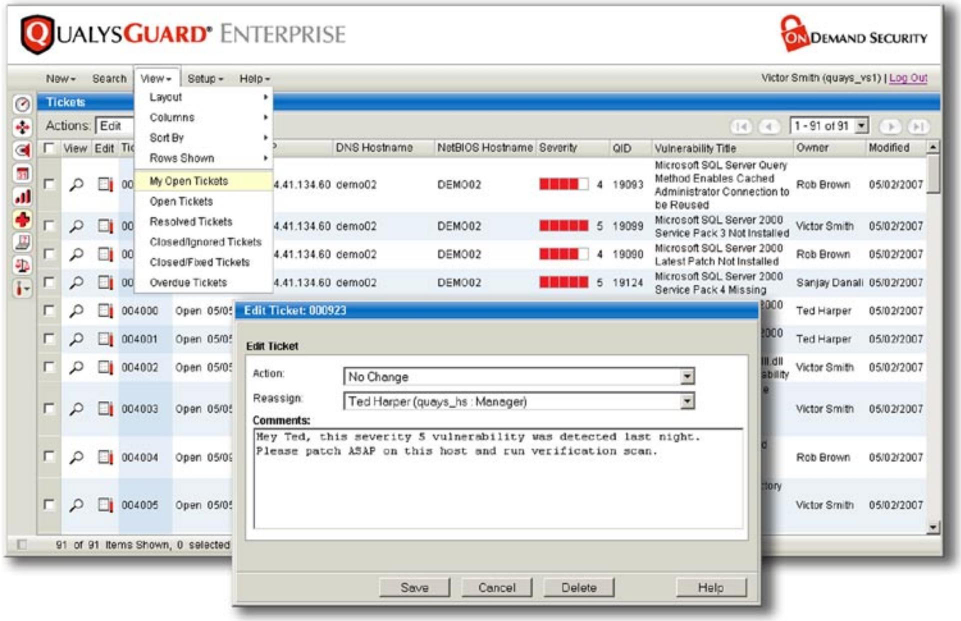
Often overlooked as a measurable IT security metric, remediation closes the loop when solving security gaps discovered during the vulnerability assessment and management process. By understanding how quickly your organization can remedy discovered vulnerabilities and misconfigurations, you gain insight into the overall security posture of your organization and its ability to put both proactive and reactive measures in place. In the wake of the reduced time between the discovery of new vulnerabilities and the availability of exploits, fast, effective detection and remediation is critical.

Remediation closes the loop when solving security gaps discovered during the vulnerability assessment and management process.

How QualysGuard Enables Effective Remediation

In addition to being able to accurately and immediately identify new vulnerabilities, QualysGuard's native ticketing and remediation system provides the visibility that organizations need to ensure that all vulnerabilities have been fully resolved, and highlights any outstanding issues that still require attention.

Through its ability to quantify your organization's mean-time-to-repair (MTTR) across business units, QualysGuard provides you the ability to fix operational performance gaps. QualysGuard's remediation capabilities can be employed as a stand-alone system, or tightly integrated with other best-in-class ticketing systems. When used in a stand-alone capacity, QualysGuard's remediation processes enable you to keep operational duties separated, while integrating it with ticketing systems could offer you additional performance measurements.



□	View	Edit	Tic		P	DNS Hostname	NetBIOS Hostname	Severity	QID	Vulnerability Title	Owner	Modified
□			00		4.41.134.60	demo02	DEMO02	■■■■□ 4	19093	Microsoft SQL Server Query Method Enables Cached Administrator Connection to be Reused	Rob Brown	05/02/2007
□			00		4.41.134.60	demo02	DEMO02	■■■■■ 5	19099	Microsoft SQL Server 2000 Service Pack 3 Not Installed	Victor Smith	05/02/2007
□			00		4.41.134.60	demo02	DEMO02	■■■■□ 4	19090	Microsoft SQL Server 2000 Latest Patch Not Installed	Rob Brown	05/02/2007
□			00		4.41.134.60	demo02	DEMO02	■■■■■ 5	19124	Microsoft SQL Server 2000 Service Pack 4 Missing	Sanjay Danali	05/02/2007
□			004000	Open 05/05						2000	Ted Harper	05/02/2007
□			004001	Open 05/05						2000	Ted Harper	05/02/2007
□			004002	Open 05/05						ll.dll sbility	Victor Smith	05/02/2007
□			004003	Open 05/05						e	Victor Smith	05/02/2007
□			004004	Open 05/09						d	Rob Brown	05/02/2007
□			004005	Open 05/05						tory	Victor Smith	05/02/2007

91 of 91 Items Shown, 0 selected

Action: No Change

Reassign: Ted Harper (quays_hs : Manager)

Comments:

```
Hey Ted, this severity 5 vulnerability was detected last night.
Please patch ASAP on this host and run verification scan.
```

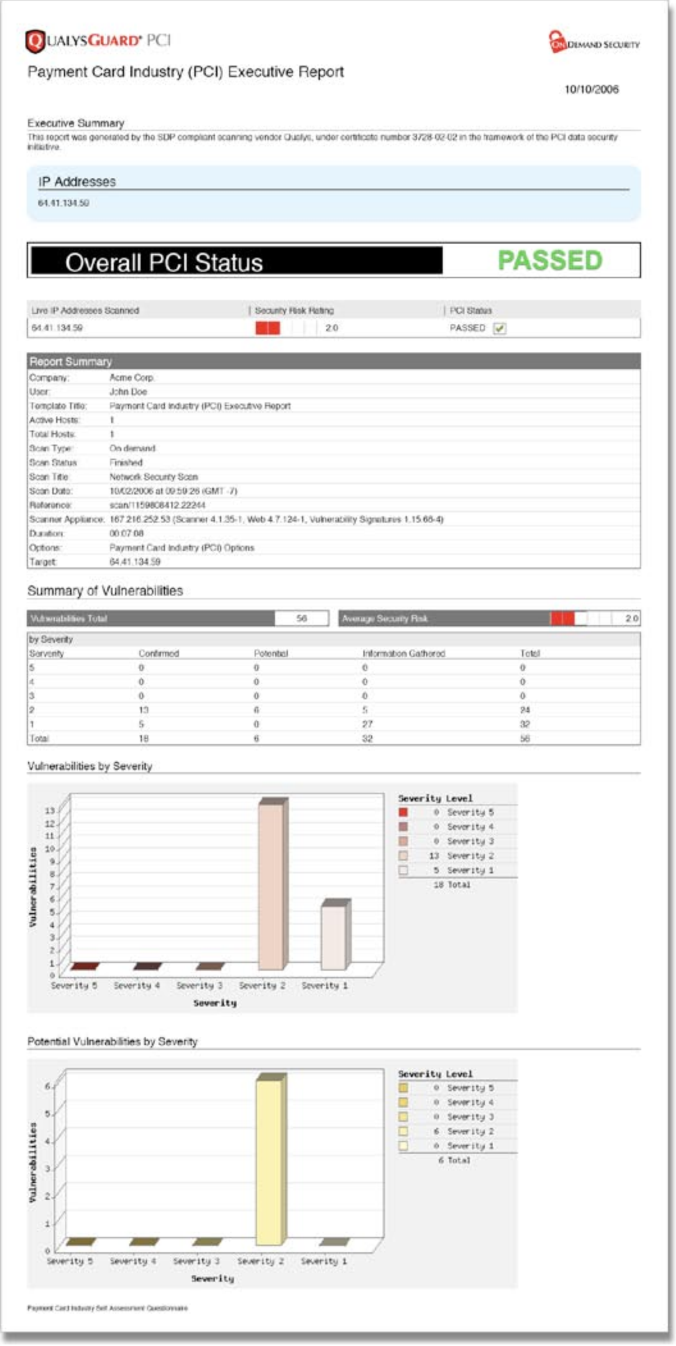
Figure 6: QualysGuard Remediation Dashboard provides a built-in ticketing and remediation tracking system.

ESSENTIAL STEP 7: Demonstrating Regulatory Compliance through Comprehensive Reporting

Maintaining regulatory compliance requires organizations be able to demonstrate that their systems are secure, and that adequate processes and procedures are in place to quickly address any gaps in security posture and compliance that may arise. For publicly traded companies, this can include detailed reports for financial systems as required by Sarbanes-Oxley. While health care organizations will need to pay special attention to clinical and administrative systems that contain private medical information in order to stay in compliance with the Health Information Portability and Accountability Act. The regulations organizations need to contend with are growing in number and complexity – FISMA, the European Directive, California SB 1386, and the Payment Card Data Security Standard (PCI DSS) – but the process and requirements are the same: substantiate adequate levels of security to industry and government regulators and auditors.

How QualysGuard Provides Powerful Regulatory Compliance Reporting

Through its ability to generate highly-customizable reports and those designed to prove compliance to common regulations, such as PCI DSS—QualysGuard provides the IT team the most effective way to demonstrate high levels of security and regulatory compliance to business managers, partners, customers, and regulatory auditors. Reports can be presented in HTML, MHT, PDF, CSV and XML formats.



QUALYSGUARD® PCI

ON DEMAND SECURITY

Payment Card Industry (PCI) Executive Report

10/10/2006

Executive Summary

This report was generated by the SDP compliant scanning vendor Qualys, under certificate number 3728-02-02 in the framework of the PCI data security initiative.

IP Addresses

64.41.134.59

Overall PCI Status PASSED

Live IP Addresses Scanned	Security Risk Rating	PCI Status
64.41.134.59	2.0	PASSED ☑

Report Summary

Company:	Acme Corp.
User:	John Doe
Template Title:	Payment Card Industry (PCI) Executive Report
Active Hosts:	1
Total Hosts:	1
Scan Type:	On demand
Scan Status:	Finished
Scan Title:	Network Security Scan
Scan Date:	10/02/2006 at 09:59:26 (GMT -7)
Reference:	scan/1159808412.22244
Scanner Appliance:	167.216.252.53 (Scanner 4.1.35-1, Web 4.7.124-1, Vulnerability Signatures 1.15.66-4)
Duration:	00:07:08
Options:	Payment Card Industry (PCI) Options
Target:	64.41.134.59

Summary of Vulnerabilities

Vulnerabilities Total 56

Average Security Risk 2.0

by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	0	0	0	0
4	0	0	0	0
3	0	0	0	0
2	13	6	5	24
1	5	0	27	32
Total	18	6	32	56

Vulnerabilities by Severity

Potential Vulnerabilities by Severity

Payment Card Industry Self Assessment Questionnaire

Figure 7: QualysGuard PCI Executive Report enables merchants to prove PCI DSS compliance.

Conclusion

With these baselines covered, security teams can turn raw security statistics into quantifiable security improvements: have the number of critical system vulnerabilities decreased over time? Have the number of IT related regulatory audit findings also been reduced? Have new processes reduced the number of days between vulnerability identification and remediation? The challenge is ensuring that your organization's ability to gather these statistics is streamlined within the daily workflow of security personnel.

The continuous measurement of your security posture and vulnerability management program is a crucial aspect of your IT security efforts. And QualysGuard enables companies of all sizes to automate the processes associated with measuring and quantifying vulnerability, compliance management, as well as IT security readiness. QualysGuard proactively provides everything needed to identify, measure, reduce, and demonstrate reduction of risk: the discovery and classification of all networked assets, identifying, prioritizing, remediation, and validation that the vulnerabilities that make the vast majority of security breaches possible have been eliminated. In addition to being able to accurately and immediately identify new vulnerabilities, QualysGuard's native ticketing and remediation system provides the visibility that organizations need to ensure that all vulnerabilities have been fully resolved, and highlights any outstanding issues that still require attention.

Through its ability to quantify your organization's mean-time-to-repair (MTTR) across business units, QualysGuard provides you the ability to fix operational performance gaps. QualysGuard's remediation capabilities can be employed as a stand-alone system, or tightly integrated with other best-in-class ticketing systems. When QualysGuard is used in a stand-alone capacity, its remediation processes enable you to keep operational duties separated, while integrating it with ticketing systems could offer you additional performance measurements that provide optimal security risk reduction.

QualysGuard enables companies of all sizes to automate the processes associated with measuring and quantifying vulnerability, compliance management, and IT security readiness.

For a Free Trial of QualysGuard, visit www.qualys.com

QUALYS®
www.qualys.com

USA – Qualys, Inc.
1600 Bridge Parkway
Redwood Shores
CA 94065
T: 1 (650) 801 6100
sales@qualys.com

UK – Qualys, Ltd.
224 Berwick Avenue
Slough, Berkshire
SL1 4QT
T: +44 (0) 1753 872101

Germany – Qualys GmbH
München Airport
Terminalstrasse Mitte 18
85356 München
T: +49 (0) 89 97007 146

France – Qualys Technologies
Maison de la Défense
7 Place de la Défense
92400 Courbevoie
T: +33 (0) 1 41 97 35 70

ON DEMAND SECURITY