QUALYS®

GUIDE

STRENGTHENING NETWORK SECURITY WITH ON DEMAND VULNERABILITY MANAGEMENT AND POLICY COMPLIANCE

Table of Contents

ON DEMAND SECURITY

QualysGuard Benefits

- **Ease of Deployment** with SaaS requires no special hardware or software – just a standard web browser.
- **Speeds Vulnerability Repairs** with automated remediation workflow for targeted action on what matters most, first.
- **Scales by Handling IP Networks of Any Size** including Class C and B networks with ease.
- **Accuracy of Scans** is Six Sigma quality. Meaning, fewer false positives or false negatives and trustworthy results.
- **Reports Measure Exposure** and risk of each vulnerability detected on the network with links to patches and problem fixes.
- **3rd Party Audit Documents Compliance** with PCI, HIPAA, GLBA, and audit rules for other regulations.
- **Comprehensive Threat Management, Lower TCO** audits vulnerabilities from a hacker's perspective at up to 90% reduction in total costs.

Network security professionals are besieged by a nonstop flood of new software vulnerabilities, easy-to-get hacker toolkits, and an army of technology criminals eager to exploit network weaknesses for fun or profit. And despite defensive efforts with firewalls, intrusion detection, antivirus and the like, criminals, careless employees and contractors have exposed more than 158 million digital records of consumers' personally identifiable information since 2005. Clearly, a more comprehensive defense-in-depth strategy is required. Core to this approach, security professionals are turning to continuous vulnerability management to find and quickly fix weaknesses in network security, and to document compliance with security and consumer privacy regulations. This security guide describes these requirements and on demand software-as-a-service (SaaS) solution called QualysGuard for effective vulnerability management and policy compliance.

Critical Need for Stronger Network Security

The risk of malicious attacks has never been higher for organizations that do not use vulnerability management to control software or configuration holes in the network. Successful exploits by hackers and criminals use viruses, worms, rootkits, phishing or other automated attack techniques in order to leverage vulnerabilities in unpatched devices and misconfigured systems.

Fallout from a successful network breach includes immediate, direct costs of repairing damage to enterprise data, systems, software and networks. Organizations may also suffer IT business system downtime, stolen intellectual property or personally identifiable information of employees, contractors and customers; exposure of business strategies or product plans; regulatory, civil or criminal penalties for non-compliance; lawsuits from customers and business partners; loss in product market share; loss in value of public stock equity; difficulty in securing new financing; and loss of trust by customers and business partners. Prudent organizations control these risks by using vulnerability management to plug holes and strengthen network security.

Recent Breaches and Data Exposure

TJX Companies exposed 45,700,000 credit card and debit card account numbers, and 455,000 records with customers' name and driver's license number.

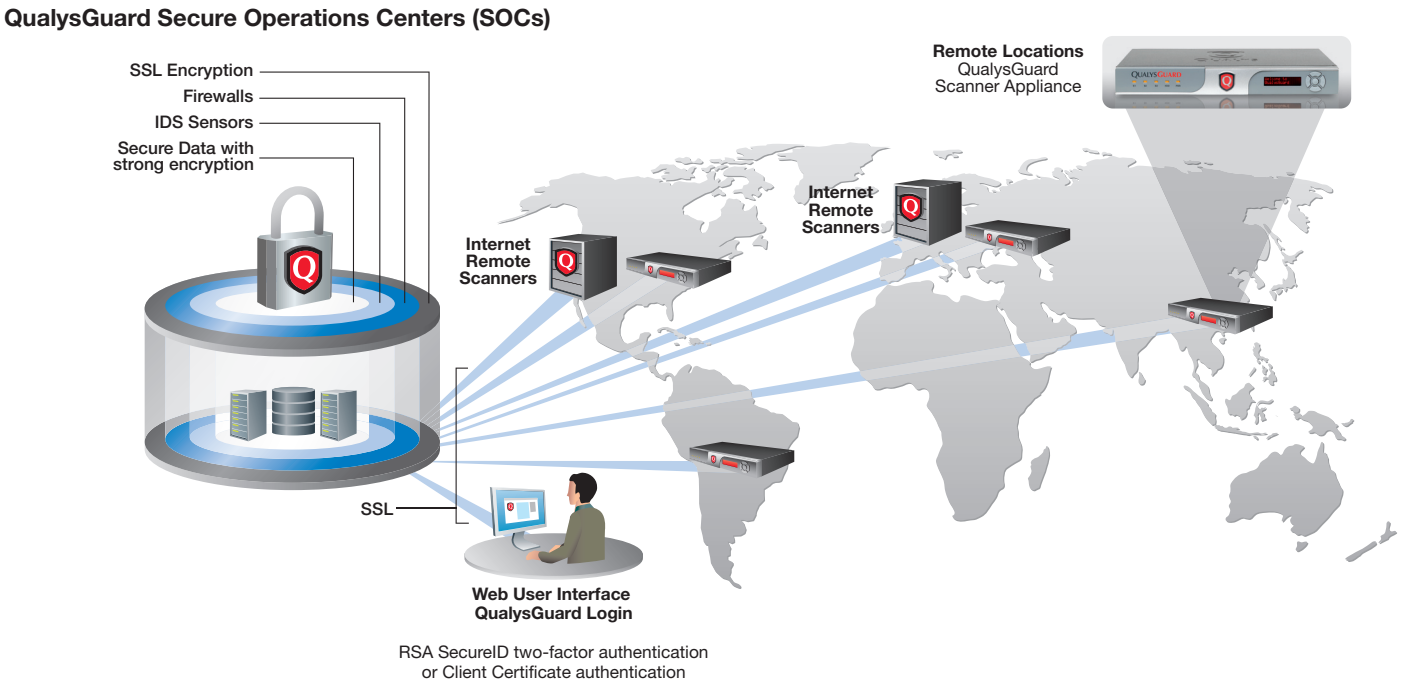
DSW Inc. exposed 1,400,000 customer credit card, debit card and checking account information.

CardSystems Solutions, Inc. exposed 40,000,000 credit card records with names, banks and account numbers.

Chicago Voter Database exposed 1,350,000 voter Social Security numbers and birthdates.

University of California – Los Angeles exposed 800,000 current and former student, faculty and staff records of name, Social Security number, home address and contact information.

QualysGuard SaaS Architecture for On Demand Risk and Compliance Management



While users simply login to QualysGuard to take advantage of the comprehensive vulnerability management system, QualysGuard's SaaS-based architecture is designed with multiple layers of data security to protect customers' vulnerability information. QualysGuard provides end-to-end security for sensitive vulnerability data, considering industry best practices at all layers of the application.

QualysGuard – SaaS-based Vulnerability Management for Stronger Security and Verification of Compliance

QualysGuard uses a software-as-a-service delivery model to automate workflow of vulnerability and compliance management. Automation is a requirement because attacks are continuous – the result of technology that automatically mutates an assault until it finds a hole that works. The SaaS secure architecture allows QualysGuard to be available for use 24x7 as often as required, scaling to any-sized network, anywhere in the world. QualysGuard allows organizations to:

Discover and manage all devices and applications on the network

By simply entering a range of IPs to be scanned into QualysGuard, it will automatically identify and map every device on all 65,536 ports in the network. The resulting map helps classify and prioritize each asset by business value. Its database can then be used on demand to identify vulnerabilities affecting specific machines by policy and configuration.

Identify and remediate network security vulnerabilities

QualysGuard automatically scans IPs on your network and matches their state to the industry's largest KnowledgeBase of vulnerability signatures, updated daily for Six Sigma accuracy. QualysGuard classifies and categorizes each vulnerability discovered on your network. Remediation workflow includes a

> *"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, Inc.**

prioritized to-do list based on IT asset values and vulnerability criteria. QualysGuard provides links to patches, fixes and workarounds for all vulnerabilities.

Measure and manage overall security exposure
Comprehensive, easy-to-understand reports quantify enterprise security posture. Technical reports guide vulnerability management and remediation. Executive dashboards present security posture in laymen's terms for non-technical managers and executives.

Ensure compliance with internal policies and external regulations
QualysGuard automatically generates reports documenting compliance with security scanning requirements of many laws, regulations and auditors, including PCI, HIPAA, GBLA, Sarbanes-Oxley, SB 1386, FISMA, the European Directive, and internal policies.

QualysGuard Benefits

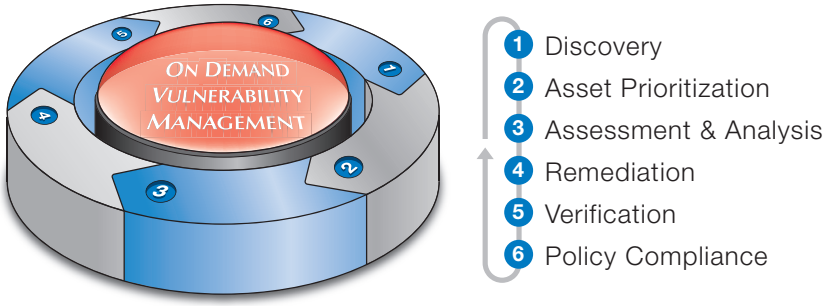
Ease of Deployment
Deploying QualysGuard is simple. Vulnerability scans and management require no special hardware or software. A standard web browser allows administrators to run role-based scans, view findings, operate remediation workflow and download patches. To ensure security, QualysGuard uses standard TCP/IP for communications plus SSL for encryption, and RSA SecureID two-factor or Client Certificate for authentication. There is no special configuration or security gurus required to do a network security audit. No training is required. Operators simply enter a range of IP addresses into QualysGuard requesting the scan and then click the "start" button. Everything is completely automated.

Speeds Vulnerability Repairs
Time is of the essence to protect networks from zero day attacks and exploits of new and old vulnerabilities alike. Security audits with QualysGuard eliminate the constant worry of overlooking a new vulnerability. An automated workflow speeds vulnerability repairs by discovering and prioritizing IP assets, finding weaknesses, ranking the severity of problems to help prioritize repair actions, and guiding remedial action with links to patches and fixes. Using on-demand vulnerability management from QualysGuard is like having an in-house, professional digital security research team correlating known configuration and patch requirements with your unique infrastructure, 24x7. QualysGuard's comprehensive audits and straightforward remediation workflow cut time by security staff to research vulnerabilities, locate problems, and apply remedies.

> *"QualysGuard 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 Corporation

QualysGuard Vulnerability Management Lifecycle



The award-winning QualysGuard solution automates and simplifies the entire vulnerability management and compliance lifecycle for any-sized organization.

Scales by Handling IP Networks of Any Size

QualysGuard does not require special network, security or other IT infrastructure. QualysGuard instantly scales to any-sized IP network simply by entering the range of IP addresses desired for a vulnerability audit. The service even handles Class C and Class B size networks with ease. QualysGuard effectively audits the security of any changes to an IP network and expands with organizational needs such as acquiring or merging with another corporation.

Accuracy of Scans

Unique advanced technology in QualysGuard provides for highly accurate scans and the virtual elimination of false positives in vulnerability reports. Inference-based scanning in QualysGuard builds a database of protocols on each machine – and only tests for vulnerabilities matching each machine's exact configuration. QualysGuard's KnowledgeBase of vulnerabilities is the largest such database in the industry. KnowledgeBase vulnerability signatures are updated daily to deliver Six Sigma accuracy — ensuring organizations are accurately testing for vulnerabilities using the most up-to-date information available. The result is unmatched scanning breadth and accuracy for every audit.

Reports Measure Security Exposure and Risk

QualysGuard automatically generates reports detailing each vulnerability identified in a scan by category and rates them via levels of severity. The severity level indicates the security risk posed by exploitation of the vulnerability and its degree of difficulty. Reports also provide security configuration advice, and hotlinks to patches and problem fixes. Security specialists may customize report formats for use by people with different roles in the organization. Executive dashboard reports enable technical specialists to present the enterprise posture of network security to non-technical business managers and executives. While technical reports satisfy the hands-on need of security professionals and administrators.

Third Party Audit Documents Policy Compliance

Fully automated vulnerability reporting by QualysGuard provides documentation for IT security compliance per the security scanning requirements of many laws, regulations, and auditors – including PCI, HIPAA, GBLA, Sarbanes-Oxley, SB 1386, FISMA, the European Directive, and others. QualysGuard automates production of concise documentation for policy compliance with report templates for key regulations. Unlike data provided by user-owned software applications, QualysGuard is trusted by auditors because it is collected and held by a secure third party. Role-based operations and reporting by QualysGuard further protect the integrity of results for verification of compliance.

Comprehensive Threat Management at a Lower Cost

QualysGuard combines the industry's largest vulnerability database with the capability to assess risks from an outside-in, hacker's view perspective. Each QualysGuard scan produces a full inventory and graphical map of all IP devices on the network, and discovers known security vulnerabilities. As a SaaS-based solution, vulnerability updates to the QualysGuard KnowledgeBase are immediately available to all subscribers worldwide for stronger network security assessment. And unlike the labor intensive and expensive costs of using a software-based solution, the SaaS-based QualysGuard solution allows users to dramatically lower total cost of operations. Customers typically need just 20% of one person's time to review reports and implement recommended fixes – the savings is up to a 90% reduction in operating costs. Comprehensive threat management is unlimited with QualysGuard so you can scan for vulnerabilities as often as you like for a fixed subscription fee.

About Qualys

Qualys, Inc. is the leading provider of on demand security risk and compliance management solutions. It is the only security company that delivers these solutions through a single software-as-a-service platform. The QualysGuard service allows organizations to strengthen the security of their networks with automated security audits, and document compliance with policies and regulations. As a scalable and open platform, QualysGuard enables partners to broaden their managed security offerings and expand consulting services. QualysGuard is the widest deployed security on demand solution in the world, performing over 150 million IP audits per year.

To learn more about 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