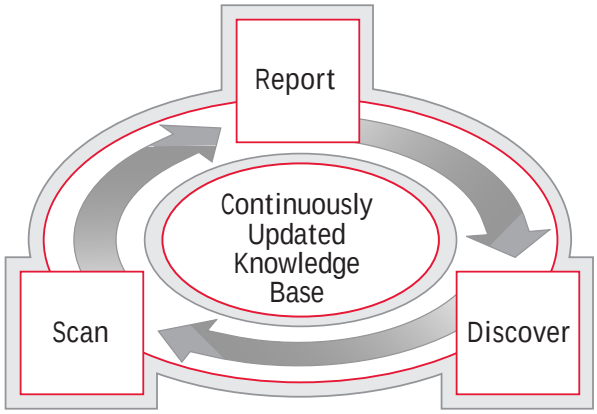
QualysGuard 2.9

QualysGuard is a highly effective, simple-to-use online service that instantly identifies and maps all the IP devices on your Internet network. It analyzes the network for potential security vulnerabilities, prepares reports on potential security risks, and helps the client to determine the most appropriate corrective measures. The service requires no installation, set-up, hardware purchases, software development, security expertise, or special training to use.

Whatever your assessment needs may be, QualysGuard provides solutions that help to identify risks against your network



BENEFITS:

- Maps your entire network topology and provides a visual representation from the "intruder's" point of view.
- Analyzes and assesses the relative risk of each vulnerability.
- Enables you to set up automatic daily updates for compiling an ongoing record of your network vulnerabilities.
- Supports a range of networks (from 0 – 265+ IP addresses).
- Requires no installation or configuration.

Visualization: QualysMap Network Topology

The QualysGuard service includes QualysMap, a unique service that instantly detects and creates a graphical map of all visible devices that can be reached via the Internet (or not reachable but reported as existing by the DNS), with access gateways, routers, operating systems, and ISP routers identification.

Analysis: Probing for Vulnerabilities

Network Administrators can choose to initiate a vulnerability analysis by selecting one registered IP address, or by entering a range of IP addresses for scanning. The Qualys Knowledge Base Scanning Engine uses an up-to-the-minute database to test for vulnerabilities on routers, switches, hubs, firewalls, Web servers, mail exchangers, UNIX and NT servers, workstations, desktop computers such as PC and Macintosh, printers, and other network appliances.

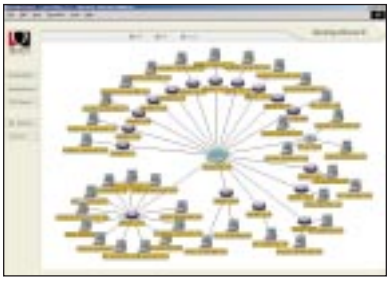
Reporting: Diagnosis, Consequences, and Solutions

QualysGuard generates easy-to-understand graphic HTML or XML reports that provide a breakdown of the security of your network devices including summary information about the scan, general network information, specific host information, and a list of detected vulnerabilities. For each detected security risk, the report presents a description of the vulnerability, the severity of the vulnerability (from 1 to 5), potential consequences of unauthorized access, and recommended solutions.

QualysGuard also generates an Executive View Report that provides a global view of the security level of all networks and IP addresses, and changes since the last scan.

All reports are stored encrypted with the user's password and therefore cannot be accessed by any other party — not even Qualys. Customer Network Administrators alone decide whether to download, keep, or delete reports from the QualysGuard database.

Easy Three-Step Process:



1 Detecting and Analyzing Areas of Vulnerability

This discovery tool uses several hacker techniques to gather information about the target domain from the DNS server, the netblock information, and from a customized version of the Traceroute program to find hosts that cannot be identified with the other methods.

2 Vulnerability Scanning

Everything with an IP address, including routers, switches, hubs, firewalls, Web servers, mail exchangers, UNIX and NT servers, workstations, desktop computers such as PC and Macintoshes, printers, and other network appliances, can be probed for vulnerabilities. For each security risk detected, the report presents a description of the vulnerability, the severity of the vulnerability (from 1 to 5), the potential consequences, and the solution recommended.

3 Global Network Overview

Management Overview: The CIO Report is designed to provide executive management with information that is at once precise and clear. It offers:

- A global view of the security level of all networks and IP addresses.
- Reports on progress since the last scan.

Technical Report: The vulnerability report provides a comprehensive analysis of vulnerabilities, the possible consequences of each vulnerability, and suggested solutions.

DEVICES SCANNED

- Routers, Administrable Switches & Hubs (Cisco, 3Com, Nortel Networks, Cabletron, Lucent, Intel, Newbridge...)
- Operating Systems (NT 3.5, NT 4.0, NT 2000, Win9x, Linux, BSD, MacOS X,Solaris, HP-UX, Irix, AIX, SCO, Novell...)
- Firewalls (CheckPoint Firewall-1, Novell Border Manager, TIS, CyberGuard, Ipchains...)
- Web Servers (Apache, Microsoft IIS, Lotus Domino, Netscape Enterprise, IpSwitch, WebSite Pro, Zeus...)
- FTP Servers (IIS FTP Server, Wu-FTPd, WarFTPd...)
- LDAP Servers (Netscape, IIS, Domino, Open LDAP...)
- Load Balancing Servers (IBM Network Dispatcher, Intel, Resonate Central Dispatch, F5, ArrowPoint, Alteon...)
- Databases (Oracle, Sybase, MS SQL, Postgresql, MySQL)
- E-Commerce (Icat, EZShopper, Shopping Cart, PDGSoft, Hassan Consulting Shopping, Perlshop...)

VULNERABILITY CATEGORIES

- DNS and Bind
- Back Doors and Trojan Horses
- Brute Force Attack
- CGI
- File Transfer Protocol
- Firewall
- MS FrontPage
- General Remote Services
- Hardware & Network Appliances
- Information Services (NIS, LDAP, WHOIS)
- SMB/Netbios Windows File Sharing
- SMTP and Mail Transfer
- Databases

Qualys, Inc.
1326 Chesapeake Terrace, Sunnyvale, CA 94089
T 408 747 6000 **F** 408 747 5255 www.qualys.com