ON-DEMAND SECURITY AUDITS AND VULNERABILITY MANAGEMENT

A Proactive Approach to Network Security

© Qualys, Inc. All Rights Reserved

Contents

© Qualys, Inc. All Rights Reserved

Executive Summary

Hacker attacks are no longer limited to high-profile organizations such as banks and governments. Automated tools have made it easier to identify and exploit network exposures, swelling the rate of attacks on networks attached to the Internet. At the same time, viruses, worms and trojans have evolved into sophisticated, self-propagating attacks resistant to detection. Newer worms complete global attack cycles and exploit vulnerable hosts in just seconds, so securing networks requires identifying and fixing vulnerabilities in advance.

"99% of network intrusions result from exploitation of known vulnerabilities or configuration errors where countermeasures were available."

Source: CERT, Carnegie Mellon University

IT groups rely on four main technologies to protect their networks: virus detection, firewalls, intrusion detection systems (IDS), and vulnerability assessment. Each has a place in a comprehensive security strategy. Only on-demand Security Audits and Vulnerability Management provide a proactive approach, identifying network and device vulnerabilities before networks are compromised.

Companies can choose from several approaches for vulnerability assessment: manual testing using software-based products, consultants' penetration testing, and self-service automated third-party solutions. With the latter approach, called on-demand Security Audits & Vulnerability Management, scans are conducted by remote servers that are hosted and maintained by a trusted third party while control over each security audit is maintained by the user. Automated security audits offer clear cost and security advantages over other methods of vulnerability assessment.

This white paper explains the value of the various approaches to network security. It focuses on the unique role of vulnerability management, and automated security audits in particular. The paper concludes with a description of the QualysGuard solution.

© Qualys, Inc. All Rights Reserved

Network Intrusions Interrupt Business, Inflict Financial Damage and Adversely Impact Customer Confidence

Following are just a few examples:

- *SQL Slammer infected more than 120,000 hosts in 10 minutes, disabling cash machines, disrupting 911 call center operations and causing widespread interruptions in Internet operations (Associated Press, 1/27/03).*
- *Microsoft IIS vulnerabilities caused credit card issuers to replace over 150,000 accounts at a cost of $5-$10 per card (USA Today, 8/10/02).*
- *Code Red and Nimda worms compromised 800,000 servers worldwide at a cost in excess of $3 billion (ABC News, 1/22/02).*
- *Hackers compromised the State of California personnel database, stealing 265,000 employees' names, Social Security numbers, and payroll information (San Francisco Chronicle, 5/25/02).*
- *About 13,000 customer records—including names, work and home addresses, Social Security numbers, account numbers, and credit histories—were stolen from Experian Information Solutions through Ford Motor Credit Company (New York Times, 5/17/02).*

The Network Security Challenge

Not too long ago, most hacker attacks targeted high-profile organizations such as banks and governments. Times have changed, and now every Internet-connected enterprise is vulnerable, whether it has thousands of IP addresses or just one.

Factors Contributing to Escalating Risk

Companies face increasing risk from network security breaches, for the following reasons:

- Networks increasingly have multiple entry points—for example, VPNs and wireless access points used by remote employees. This exposes networks to threats from unknown software and unprotected connections.
- Networks and applications have grown more complex and difficult to manage, even as qualified security professionals are scarce and IT budgets have come under pressure.
- Compressed software development lifecycles result in flawed or poorly tested releases. As a result, the number of newly discovered and exploitable vulnerabilities has grown 1,149 percent in the past five years.
- Hacking tools have become automated and require less skill to use, increasing the ranks of hackers. And because these tools are automated and designed for large-scale attacks, a single hacker can rapidly inflict widespread damage. (see Figure 2: CERT Security Incident Reports)
- Malicious self-propagating worms, viruses, and trojans boost damage through a multiplier effect: they keep on "giving" long after the initial incident.
- The lifecycle for network attacks is shorter (see Figure 1: Accelerating Vulnerability and Exploit Lifecycle). Therefore, companies have less time to identify and correct vulnerabilities before they are exploited by hackers and worms.

© Qualys, Inc. All Rights Reserved

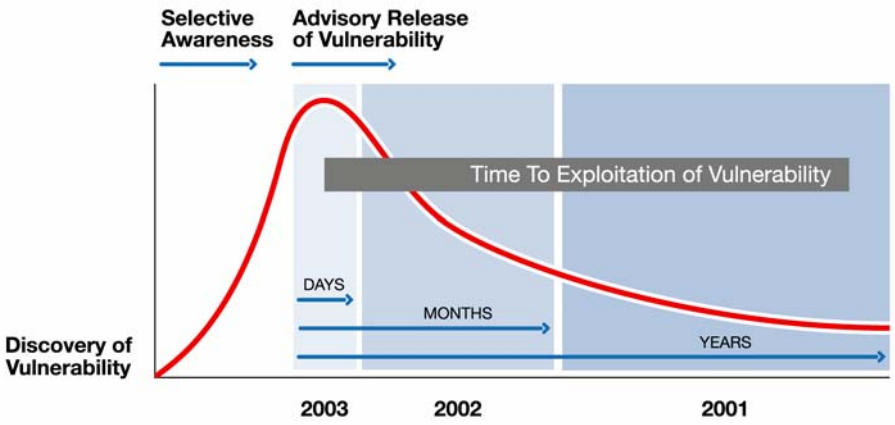

Figure 1—Accelerating Vulnerability and Exploit Lifecycle
The window of exposure between a vulnerability emerging and being exploited is narrowing from weeks to just a few days. Early detection is key to preventing intrusion and compromise of data assets.

Prevalence and Consequences of Security Breaches

The 2003 Computer Crime and Security Survey, conducted by the Computer Security Institute (CSI) and the San Francisco Federal Bureau of Investigation's (FBI) Computer Intrusion Squad, reported the following results from a small survey of 530 large corporations and government agencies:

- 92% of respondents had detected computer security breaches within the last 12 months.
- 75% of those acknowledged financial losses due to computer breaches.
- 47% (251 respondents) quantified their financial losses: a total of $201,797,340 – with the most serious financial losses occurring through theft of proprietary information or denial of service.
- 78% identified their Internet connection as a more frequent point of attack than their internal systems.
- Only 30% reported intrusions to law enforcement agencies; most did not to avoid potential risks of negative publicity and competitors using the information to their advantage.

As a consequence of these trends, companies must be increasingly vigilant to protect their networks from surging numbers of vulnerabilities that can be exploited by worms and automated attack methods.

© Qualys, Inc. All Rights Reserved

Growing Costs

The threat from hacking is rampant. The Computer Emergency Response Team (CERT) reports that the number of "security incidents" filed at its coordination center at Carnegie Mellon University rose 1,149 percent from 1999 through 2003[1] – an average annual compounded rate of 65.7 percent. (CERT defines an incident as an "attempt, either failed or successful, to gain unauthorized access to a system or its data.") Each such attempt represents a potential threat to corporate system data integrity, service availability, and information confidentiality.

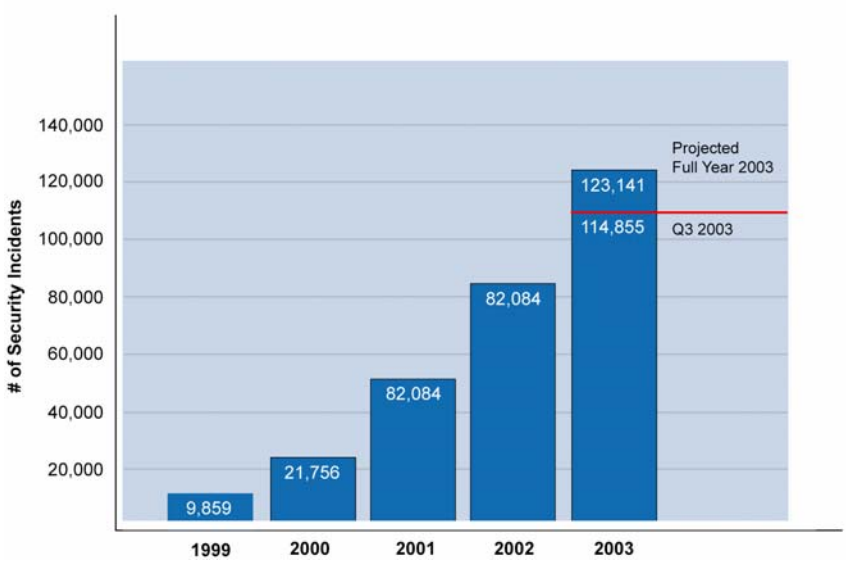

Figure 2—CERT Security Incident Reports
Annual intrusions are growing geometrically.

The cost of security breaches measures in the billions of dollars: in downtime, repairs, siphoning of IT resources, and incalculable damage from loss of customer confidence. The ultimate cost of network security failures can be loss of business. Online retailer Egghead.com ceased operations less than a year after it discovered that a hacker had accessed its computer systems, forcing it to turn over to issuing banks the names of 3.7 million credit card holders whose data might have been compromised.

[1] Assumes a projected growth rate of 50 percent from 2002 through 2003 for unaccounted Q4 data; growth through Q3 was 40 percent.

© Qualys, Inc. All Rights Reserved

Gartner Recommends Vulnerability Management

Security Demands Drive Shift to Vulnerability Management

"Enterprises that practice sound vulnerability management, rather than only intrusion detection, will experience fewer cyberattacks and suffer less damage from them."

M. Nicolett, J. Pescatore (11/19/2003)

Yankee Recommends Vulnerability Management

Vulnerability Management: Processes Strengthen IT's Security Performance

"The Yankee Group recommends vulnerability management services for enterprises that would incur financial risk if their network or key business applications were to become unavailable due to a misconfiguration or cyberattack.."

Eric Ogren (12/10/2003)

The "Four Pillars" of Network Security

Companies can take advantage of a combination of strategies to ensure network security: virus detection, firewalls, intrusion detection systems (IDS), and vulnerability assessment. All four play distinct, important roles.

Most organizations have deployed firewalls that deny unauthorized network traffic. Some organizations have also deployed intrusion detection systems. And virtually all organizations have anti-virus solutions. With all these security technologies, how do intruders continue to successfully penetrate networks and create havoc? The answer: by exploiting the vulnerabilities of the applications that organizations employ to run their businesses. Therefore, identifying and correcting these vulnerabilities before they can be exploited is an operational necessity.

The following table lists the four major approaches to network security, their function and their limitation when used alone.

Security Approach	Description	Limitation When Used Alone
Virus detection	Monitors local and server file systems and memory, and email servers for viruses; effectively stops viruses from entering a network or system.	Does not close or resolve open vulnerabilities exploited by hackers, script-kiddies, worms and automated attacks.
Firewall	Ensures that communications between a company's servers and the outside conform to specified security policies. Also acts as an authentication point for users and often a VPN end-point between networks or with remote users.	Generally configured to allow HTTP, FTP and SMTP network traffic, often the optimal path for vulnerability exploitation. Also, firewall policy changes can expose hidden vulnerabilities.
Intrusion Detection System (IDS)	Notifies administrator of possible hacking attempts when anomalous activity occurs.	Does not inform network administrator of vulnerabilities before they are exploited, when action is most valuable. Is prone to false positives, false negatives and requires complex configuration.
Vulnerability Assessment	Enables companies to identify and correct vulnerabilities before they are exploited, by testing network devices and systems for weaknesses, identifying vulnerability locations; and providing verified remedies for managed resolution.	Informs network and system administrators of vulnerabilities and remedies. Does not inform administrators when break-ins occur or perform cleansing of virus-infected files, leaving these tasks to IDS and anti-virus tools.

Table 1—Four Pillars of Security
Virus detection, firewalls, IDS, and vulnerability assessment represent four distinct network security technologies. Each is useful; none is a complete solution.

© Qualys, Inc. All Rights Reserved

CERT Recommends Vulnerability Assessment

CERT states that vulnerability assessment improves computer security by detecting rogue systems and monitoring for new access points.

- "Periodically execute vulnerability scanning tools on all systems to check for the presence of known vulnerabilities…and eliminate all vulnerabilities identified by these tools."
- "Periodically execute network mapping and scanning tools to understand what intruders who use such tools can learn about your networks and systems."

Virus Detection

Anti-virus software operates on file servers and desktops to monitor file systems and memory for patterns that indicate the presence of a virus. Anti-virus software also operates on email-servers, the entry point for almost 90 percent of viruses. Virus detection requires frequent or automated updates for accuracy. However, new multi-part worms—containing a self-propagating outer layer that exploits vulnerabilities to circumvent security systems and an inner layer "payload" that might have a malicious viral component—like Code Red—avoid anti-virus methodologies by exploiting application vulnerabilities. When anti-virus tools were updated to cleanse Code Red from systems and networks, the same vulnerability exploited by Code Red was soon used by Nimda—the identical open door used twice. Identifying and resolving vulnerabilities clearly requires a technology other than anti-virus tools.

Firewalls

Firewalls serve as security beachheads that define the network perimeter where an enterprise meets the Internet. Because firewalls determine what traffic is allowed to pass into an enterprise from the Internet, they are the essential first line of defense against hackers. A firewall that is a perfect brick wall admits no outside traffic and ensures perfect security for an enterprise. It is hardly practical, however, because it isolates the company from its customers and partners. Rather, the firewall must selectively admit traffic based on the guidelines a company defines. This opens the door for potential intruders. What's more, whenever the company modifies its firewall policies—for example, to permit new services or devices to access the Internet, or to update policy—it might inadvertently create new security vulnerabilities.

Intrusion Detection Systems

Intrusion detection systems (IDS) monitor and analyze system and network events to find and warn network administrators of unauthorized attempts to access system resources. With IDS, an organization discovers hacking attempts or actual break-ins by analyzing its networks or hosts for inappropriate data or other anomalous activity.

There are two approaches to IDS:

- Host-based IDS operates by monitoring hosts for suspicious activity. The monitoring often takes place at the file or operating system level, usually via additional software that runs on the monitored host. For example, a monitoring process might scrutinize system logs, files or other resources for unexpected changes, and raise alarms or other notifications when it detects unusual activity. Host-based IDS products are installed atop a host's operating system; they intercept and validate software and user calls made into the operating system and kernel.

© Qualys, Inc. All Rights Reserved

- Network-based IDS operate by monitoring network packets as they pass across the network. This type of solution can be implemented in hardware or software. Network-based IDS can also detect when worms compromise systems by “seeing” the worm try to propagate itself from the host.

IDS solutions play a valuable role as rearguard sentries. That is, they raise alerts that an attack may be taking place. However, corporate information security professionals would naturally prefer to prevent attacks rather than learning that they have already occurred. Other limitations of IDS include:

- Insufficient data—The data present in the network packets or system calls often isn’t enough to determine conclusively whether an intrusion is taking place.
- Flawed processing assumptions—When network IDS are located in a demilitarized zone (DMZ) or on outward-facing networks, they might interpret behavior as belligerent that is, in fact, harmless to the inside facing, protected networks. For example, a malformed packet received on an outside network isn’t necessarily capable of inflicting damage on protected networks.
- Throughput issues—Both host-based and network-based IDS are required to filter or examine large quantities of data. Today’s networking equipment often runs at speeds of 100 Mbps or greater and can overwhelm the processing capability of IDS products, which often lack sufficient throughput to examine all data.
- Active evasion—Hackers most often initiate this type of attack by subtly rewriting packets to confuse the IDS. Among the techniques attackers use are denial of service attacks, so-called “insertion” attacks that create false-positives in the IDS, and “evasion” attacks that slip past the IDS to wreak havoc on the target system.

Vulnerability Assessment

IDS is reactive, detecting attacks while or after they occur. Vulnerability assessment is proactive, determining susceptibility to attacks before networks are exploited. With early vulnerability detection, companies can take corrective action before damaging network attacks can take place. Vulnerability assessment has traditionally been conducted with techniques such as annual or quarterly penetration testing by expert consultants. Now, with on-demand security audits and vulnerability management, organizations can detect and eliminate vulnerabilities frequently and at a reasonable cost, closing their networks’ windows of exposure.

Vulnerability assessment is a methodical approach to identifying and prioritizing vulnerabilities, enabling IT organizations to non-intrusively test their networks from the “hacker’s perspective” and automatically:

- Identify vulnerabilities and network misconfigurations.

© Qualys, Inc. All Rights Reserved

- Identify rogue devices, including wireless and VPN-access points.
- Detect and prioritize vulnerability exposures.
- Provide remedies for known vulnerabilities.
- Validate firewall and IDS configurations.

Companies that perform vulnerability assessment typically scan new systems when they are attached to the network, after software is installed or reconfigured, and at regular intervals thereafter. When a vulnerability is detected, the company corrects it and then performs another scan to confirm that the vulnerability is gone.

Vulnerability assessment works hand in hand with anti-virus, firewall, and IDS. The vulnerability assessment identifies potential vulnerabilities before they can be exploited, and the intrusion detection system notifies the company when anomalous activity has occurred. The two approaches are synergistic: vulnerability assessment enables IT to identify and close obvious holes so that the intrusion detection system produces a manageable volume of alerts.

Vulnerability assessment also works in conjunction with firewalls to continuously and seamlessly monitor for vulnerabilities that may have inadvertently been introduced by firewall policy changes.

The process of vulnerability management incorporates a combination of processes and technologies which includes asset discovery, vulnerability assessment, analysis of audit results, and the management of corrective actions/remediation.

© Qualys, Inc. All Rights Reserved

Gartner Recommends Near Continuous Scanning

"Near continuous scanning is needed to quickly identify new vulnerabilities because application, network and system changes invariably introduce configuration errors, and new vulnerabilities are frequently announced by system and application vendors. Because cyberattackers are continually scanning for openings, enterprises need to find these vulnerabilities before the attackers do."

M. Nicolett, J. Pescatore (11/19/2003)

Comparing Approaches to Vulnerability Assessment

Companies can choose from several approaches to vulnerability assessment: manual testing using software-based products, consultants' penetration testing, and externally hosted self-service automated solutions. With the latter approach, also called on-demand security audits, scans are conducted remotely by a third-party service while complete control is maintained by the user. Using an external service approach is the only way to obtain unbiased third-party audits of security – both for finding and fixing actual weaknesses, and for documenting compliance with federal and state security regulations.

Product-Based vs. Service-Based Solutions

There are two categories of vulnerability assessment solutions: product-based and service-based.

Product-Based Solutions

Product-based solutions are installed on the enterprise's internal network, and are generally manually operated. The drawback of the product-based approach to network vulnerability assessment is that it fails to deliver an outside view of the network's weaknesses. The product must be installed on either the non-routable, or private portion of an enterprise network or on its openly Internet-addressable portion. Both installation options pose problems. If the product is installed on the private portion—that is, behind a firewall—then it cannot always detect the many varieties of outside attacks that involve explicit delivery of malformed packets to the targeted enterprise network. The firewall itself, whether proxy-based or packet-based, distorts the accuracy of the resulting test, and false-positives and false-negatives abound.

If the product is installed on a public, Internet-addressable network, the security of the node running the vulnerability assessment software becomes a major concern. What happens if the machine performing vulnerability testing is itself attacked or monitored? How are the results securely communicated from the outside host to secure nodes? The company risks not only a corrupt assessment, but also exposing vital information on internal networks to hackers.

© Qualys, Inc. All Rights Reserved

Thinking Like a Hacker

QualysGuard mimics the hacker workflow. Each scan involves the following steps:

- *Information Gathering — Finding out as much about a host as possible without visiting or connecting to it, with techniques such as whois, DNS, and IP assignments.*
- *Discovery—Identifying hosts in the target subnet (topology, firewalls, and other devices).*
- *Scanning—Finding out the potential targets and vulnerabilities associated with hardware, software, and their open ports via network scanning and port scanning.*
- *Correlating—Confirming the vulnerabilities to achieve the goal.*

A further shortcoming of product-based vulnerability assessment occurs when testing large networks. Large networks invariably require multiple nodes running the vulnerability assessment software. The results of the analysis are then, naturally, dispersed across multiple machines. In order to provide an enterprise-wide view, administrators typically must collate the data and produce report results manually, an additional chore for already overworked security administrators.

A final consideration is maintenance. Software needs to be updated to scan for the latest vulnerabilities. With dozens of new vulnerabilities discovered each week, remaining current imposes another time burden on administrators.

Service-Based Solutions

Third parties offer service-based solutions. Some service-based solutions are network hosted, while others are externally hosted. The latter type of solution mimics the perspective of a hacker to audit a network at its perimeter. That is, the assessment is initiated from the hacker's point of view: from the outside, looking in. Service-based solutions are offered both by outside consultants and by providers of automated security audits, such as Qualys (see sidebar: Thinking Like a Hacker). Third-party audits should also include the capability to assess the security of internal networks inside the firewall perimeter. To securely detect internal weaknesses, service-based solutions utilize hardened appliances to accurately test within the corporate firewall. Combining the external and internal information gives organizations a 360 degree view of all potential threats.

Tree-Based vs. Inference-Based Assessment

Whether product-based or service-based, vulnerability assessment tools employ either tree-based or inference-based assessment technology.

Tree-Based Assessment Technology

Early vulnerability assessment technologies relied on lists, or trees, of vulnerabilities to test against a server or device. Administrators provided the intelligence by selecting the trees appropriate for each machine—for example, the trees for a server running Windows, Web services and a database.

This approach to vulnerability assessment relies on administrators to provide an initial shot of intelligence, and then the scan continues blindly, without incorporating any information discovered during the scan. Furthermore, all of the tests in a given tree are attempted, regardless of whether they are appropriate for the configuration of the devices being tested. Consequently, testing takes longer and the hosts tested are placed under additional, unnecessary load.

Inference-Based Assessment Technology

Inference-based vulnerability assessment technology provides an approach that differs considerably from the tree-based approach described above.

© Qualys, Inc. All Rights Reserved

With inference-based assessment, the scanning process begins by gathering information based on discovery methods, including host identification, operating system detection and fingerprinting, port scanning, and protocol detection. Information obtained through discovery enables the scanning engine to determine which ports are attached to services, such as Web servers, databases, and e-mail servers. After the intellligence gathering phase, the scanning engine intelligently selects and runs appropriate vulnerability checks for the scan. Only vulnerabilities that could be present on each machine's configuration will be tested.

Inference-based scanning is an expert systems approach that learns information about a system in exactly the same fashion that a hacker would. Inference-based assessment systems integrate new knowledge as it is discovered. This knowledge is used to build intelligence on the machine in real-time and to run precisely the tests that are likely to produce results. Therefore, this approach is more efficient, imposes less load on the machine, and maximizes vulnerability discovery while minimizing false-positives and false-negatives.

Criteria for an Effective Vulnerability Assessment Solution

The most effective vulnerability assessment solution meets the following criteria:

- Identifies perimeter and internal weaknesses from an objective, trusted, third-party perspective.
- Automatically scans against a continually updated, comprehensive database of no attack methods.
- Highly accurate vulnerability detection and elimination of false-positives using non-intrusive methods.
- Inference-based scanning engine that selectively tests for applicable vulnerabilities. This intelligent approach to vulnerability assessment ensures that only applicable vulnerabilities are tested for each scan.
- Harnesses the Web as a deployment system, enabling:
  - 24x7 auditing, both scheduled and on-demand.
  - Accessibility from any Web browser.
  - Scalability as the network grows.
  - Distributed scanning for all locations.
  - Auto-provisioning for ease of adding/removing devices and users.
  - Elimination of software installation and maintenance.
- Generates concise, actionable, customizable reports, including prioritization of vulnerabilities by severity level and trend analysis.
- Provides tested remedies and workarounds to correct vulnerabilities.
- Supports heterogeneous networks.

© Qualys, Inc. All Rights Reserved

Highlights of QualysGuard Subscriber Benefits

Designed to operate effectively on heterogeneous networks of any size, QualysGuard is the first scalable, cost-effective Web service providing proactive on-demand security audits inside and outside the firewall. QualysGuard enables total control over the security audit and vulnerability management process, including:

- Scalable management based on the Qualys Web Services Architecture
- Fully-automated solution eliminates traditionally labor-intensive operations, saving time and simplifying large-scale vulnerability management
- Rapid identification and visualization of network assets
- Accurate vulnerability detection eliminates the time-consuming, manual work of verifying results and consolidating data
- Accessible to authorized users from anywhere on the globe

QualysGuard On-Demand Security Audits and Vulnerability Management

QualysGuard ushers in the next generation of inference-based scanning technology. As a user-run, remotely hosted and managed Web service, QualysGuard automates network security audits and vulnerability management – dramatically improving the effectiveness and efficiency of network security professionals. The Web service mimics the "outside, looking in" perspective of a hacker to audit a network inside and outside the firewall.

QualysGuard is a subscription-based service that allows customers to initiate an unlimited number of scans, either scheduled or on-demand, from any Web browser. Because the subscription price is based on the number of IP addresses scanned, network administrators can run as many scans as necessary, whenever required, to identify vulnerabilities and confirm that remedies were successful. QualysGuard is also available on a pay-per-scan basis. For security consultants, a QualysGuard Consultant offering is available as well.

Companies that subscribe to the QualysGuard service gain the objective perspective of a third party, automatically identifying vulnerabilities for which they might not have thought to test, and complying with industry-specific regulations for network security and corporate governance, such as the U.S. Healthcare Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA) affecting U.S. financial service providers, the Sarbanes-Oxley Act, California SB 1386, the Turnbull Report on Internal Control for public companies in the UK, and the UK's Data Protection Act.

Qualys provides a trusted and objective third-party service. QualysGuard requires no installation, set-up, software purchases, maintenance, in-house security expertise, or special training. QualysGuard automates the vulnerability assessment process (see Figure 3: QualysGuard Provides On-Demand Security Audits and Vulnerability Management). Unlimited scans allow network administrators to conduct any number of network audits and to reassess vulnerabilities every time a device is changed.

The following sections summarize QualysGuard's security audit service components, all of which are included with the subscription.

© Qualys, Inc. All Rights Reserved

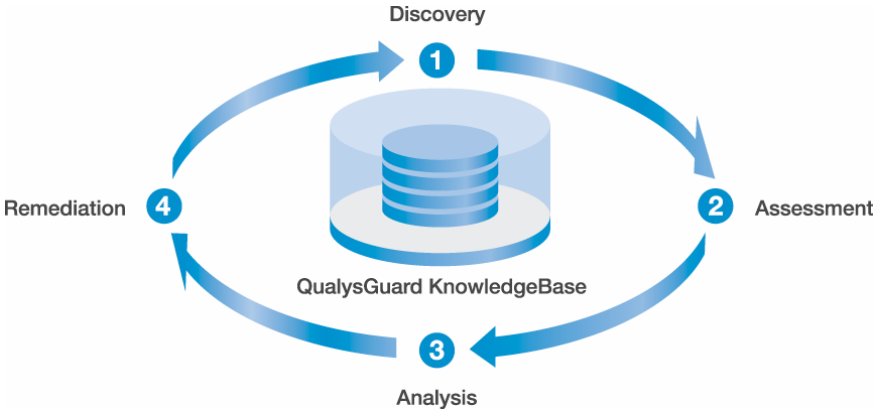

Figure 3—QualysGuard Provides On-Demand Security Audits and Vulnerability Management
With each scan, QualysGuard discovers and maps network devices, analyzes them against the industry's most comprehensive and up-to-date database of vulnerabilities using an inference-based approach. QualysGuard also provides clear, indelible audit reports with links to proven remedies and workarounds.

Audits and Manages Vulnerabilities Inside and Outside the Firewall

QualysGuard lets organizations check security from an outsider's perspective. By virtue of its Web Services Architecture (see Appendix 1), QualysGuard Intranet Scanners look in on the organization's network from outside the firewall. QualysGuard automatically audits all the organization's hosts facing the Internet. Appliance versions of Qualys Remote Scanners enable internal network auditing. Qualys Intranet Scanners easily snap in to an organization's network and allow QualysGuard to securely scan for internal vulnerabilities. The appliance is fully automated with the latest vulnerability signatures and requires no maintenance. It employs secure communications with SSL encryption and allows you to scan a distributed network with multiple locations while centralizing all reporting.

Discovery: Dynamic Identification of All Network Devices

QualysGuard creates an accessible inventory of all devices and systems on the network, and produces a visual topology of all of an enterprise's networked devices that can be "seen" from the Internet (see Figure 4: Network Discovery). By performing full ping sweeps of IP addresses and fingerprinting hosts, QualysGuard accurately discovers and maps:

- Access gateways, routers, operating systems, and ISP identification for each host.
- Customer network span.
- Access points to the discovered networks.

© Qualys, Inc. All Rights Reserved

How QualysGuard Finds Hosts

Qualys uses the following methods to identify hosts:

AXFR: QualysGuard identifies the name server (NS) that has authority on the domain and sends a request to list all the hosts managed by the server. However, this request is not always allowed. In fact, administrators should and typically do configure systems to deny such requests.

FQDN Brute Forcing: QualysGuard uses a proprietary list of roughly 100 common hostnames (for example, www, ftp, etc.) to form a list of fully qualified domain names (FQDNs). QualysGuard then queries the NS to find the IP addresses assigned to the FQDN.

Ping Sweep: QualysGuard pings address ranges provided by the administrator to find target hosts.

- Machine names.
- Private networks and intranets.
- Common open TCP ports.
- Operating systems for each host discovered.

Sometimes QualysGuard identifies devices that the network administrator did not know were on the network—including hosts that may have been maliciously or accidentally placed on a network.

All map results are encrypted and stored for later retrieval and differential reporting so once a baseline architecture is established, comparative mapping can help track rogue systems. Subscribers can execute an unlimited number of network maps, scheduled or on-demand, thus constantly monitoring network architecture and comparing configurations over time.

To use the discovery service, the customer submits one or more domain names and a set of network IP address ranges to QualysGuard. QualysGuard then uses this information to find computers within that domain and address space that can be accessed via the network. Administrators can use this information to locate devices outside the DNS record as well as to validate firewall and IDS configurations. (See sidebar: How QualysGuard Finds Hosts.) Network topology reports are provided in three forms—graphical, XML, and tabular HTML.

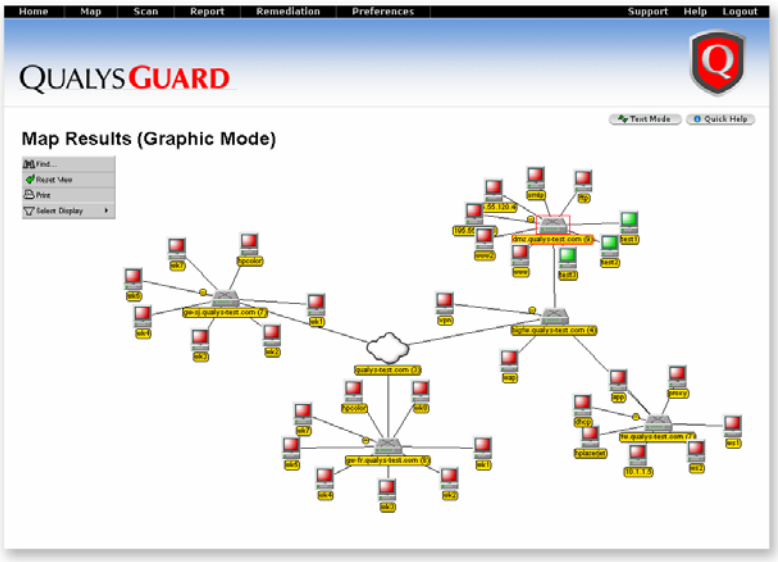

Figure 4—Network Discovery
QualysGuard instantly identifies all devices on the Internet perimeter and inside the firewall, and maps their topology. Differential mapping is available on-demand so network administrators can detect rogue systems.

© Qualys, Inc. All Rights Reserved

Devices and Applications Scanned by QualysGuard

Operating Systems:
Windows NT and 2000, Linux, BSD, MacOS X, Solaris, HP-UX, Irix, AIX, SCO, Novell

Web Servers:
Apache, Microsoft IIS, iPlanet, Lotus Domino, IpSwitch, Zeus; and full support for virtual hosting

SMTP/POP Servers:
Sendmail, Microsoft Exchange, Lotus Domino, Netscape Messaging Server

FTP Servers:
IIS FTP Server, WuFTPd, WarFTPd

Firewalls:
Check Point VPN-1/FireWall-1 and NG, Cisco PIX, NetScreen, Gauntlet, CyberGuard, Raptor

Databases:
Oracle, Sybase, MS SQL, PostgreSQL, MySQL

eCommerce:
Icat, EZShopper, Shopping Cart, PDGSoft, Hassan Consulting Shopping, Perlshop

LDAP Servers:
Netscape, IIS, Domino, Open LDAP

Load Balancing Servers:
Cisco CSS, Alteon, F5 BIG IP, IBM Network Dispatcher, Intel Routers, Administrable

Switches, and Hubs:
Cisco, 3Com, Nortel Networks, Enterasys Networks (Cabletron), Lucent, Alcatel

Analysis: Inference-Based Vulnerability Scanning

QualysGuard analyzes each networked device and system for possible vulnerabilities using a proprietary inference-based methodology. Its expert systems analytics "learn" the topography of networks it is scanning, making no assumptions or eliminations without a complete understanding of each system under test – ensuring accurate and complete detection. Assessments include active tests, protocol and daemon fingerprinting, brute forcing and password guessing, as well as network and application layer testing. (See Figure 5: QualysGuard's Inference-Based Scanning Engine.) To initiate the analysis, the administrator selects a host or hosts by OS type, location, functional group, network administrator, etc. to scan from the QualysGuard Web page. Subscribers are entitled to an unlimited number of scans, which can be scheduled or run on-demand.

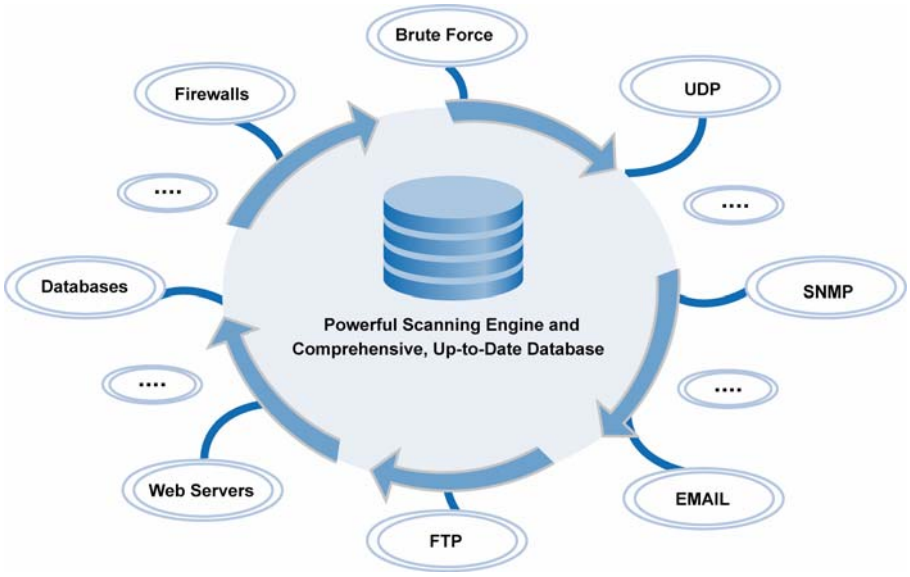

Figure 5—QualysGuard's Inference-Based Scanning Engine
QualysGuard conducts audits using an adaptive process that intelligently runs only tests applicable to the host being scanned, from a library of hundreds of proprietary test modules, thus optimizing the scanning process and minimizing the traffic load on clients' networks.

The impact of scans on network load is nominal because QualysGuard's inference-based scanning engine tests only those exploits that match the configuration of the network. For example, Qualys will not test Windows-NT vulnerabilities on a Linux machine. For more efficiency, QualysGuard continuously samples available bandwidth and utilizes only the fixed percentage specified by the network administrator.

The comprehensive QualysGuard Scanning Engine references a continuously updated Vulnerability KnowledgeBase that includes thousands of unique network vulnerability audits. The KnowledgeBase is the backbone for a QualysGuard – scanning networks, systems, applications, commercial and open source operating systems. As vulnerabilities

© Qualys, Inc. All Rights Reserved

Vulnerability Categories Covered by QualysGuard

Back Doors and Trojan Horses

Brute Force Attacks

CGI

Databases

DNS and Bind

eCommerce Applications

File Transfer Protocol

Firewalls

General Remote Services

Hardware and Network Appliances

Information/Directory Services

SMB/Netbios Windows

File Sharing

SMTP and Mail Applications

SNMP

TCP/IP

Web Servers

X-Windows

emerge—an average of 25 each week—signatures are created and immediately installed in the KnowledgeBase, so QualysGuard subscribers are automatically scanning for the latest known vulnerabilities. For the latest security vulnerability count and description of recent vulnerabilities detected please go to http://www.qualys.com/research/rnd/knowledge/vulncount/.

A vulnerability assessment system is only as strong as the database of exploits for which it is testing. Qualys does not believe in a "single source" approach to vulnerability and exploit data acquisition. The Qualys KnowledgeBase combines vulnerability and fingerprint data from numerous sources, including Qualys partner Security Focus (Bugtraq) as well as additional information collected from CERT, CVE, hacker Internet sites, underground mailing lists and numerous others.

The centralized QualysGuard KnowledgeBase is updated continually, often several times daily. Updates are automatically made available to all subscribers simultaneously. The KnowledgeBase continually feeds the latest audits to the Qualys scanning servers, ensuring that users of the QualysGuard system are always testing for the latest vulnerabilities.

Like topology maps, all scan results are encrypted and stored for later retrieval and dynamic reporting, including trend analysis.

In summary, QualysGuard's unique Scanning Engine is:

- Non-intrusive, with no impact on the availability or integrity of hosts being scanned.
- Inference-based scanning engine is modular, so that only applicable vulnerabilities are tested based on intelligent information gathering during the scan process. Host discovery methods, port scanning, OS detection and fingerprinting, and protocol discovery methods are employed.
- Accurate and complete, performing:
  - Banner identification and active tests.
  - Protocol and daemon fingerprinting.
  - Brute forcing and password guessing.
  - Network and application layer testing and analysis.
- High performance and scalable – able to scan distributed networks with thousands of devices.

© Qualys, Inc. All Rights Reserved

Severity Levels

The QualysGuard Scanning Engine assigns a severity level to each vulnerability detected:

- *Level 1 (minimal): Information can be collected.*
- *Level 2 (medium): Sensitive information can be collected, such as precise version and release numbers of software running on the target machine.*
- *Level 3 (serious): Indications of threats such as directory browsing, denial of service, or partial read of limited files have been detected.*
- *Level 4 (critical): Red-flag indications of file theft, potential backdoors, or readable user lists present on target machines have been discovered.*
- *Level 5 (urgent): Read and write access on files, remote execution, backdoor software detected, or other activities are present.*

Reporting: In-Depth Technical or Summary Data and Trend Analysis

QualysGuard delivers both technical data and summary data, in customizable or pre-defined formats. Graphical reports can be generated in HTML using the QualysGuard Web user interface (see Figure 6: QualysGuard Vulnerability Report). Reports summarize the security status of each network device, including information about the scan, specific host information, and a list of detected vulnerabilities. These reports present a description of each security risk detected, the severity of the threat (industry standard ratings from 1 to 5), the potential consequences of exposure, and links to validated patches and fixes (see sidebar: Severity Levels). Armed with this information, security managers can prioritize where and how to take corrective action.

Based on scanning history, QualysGuard also produces trend analysis and differential reports on security policy compliance. Managers and executives can take advantage of this information to allocate budgets and update insurers, business partners, shareholders, and boards of directors.

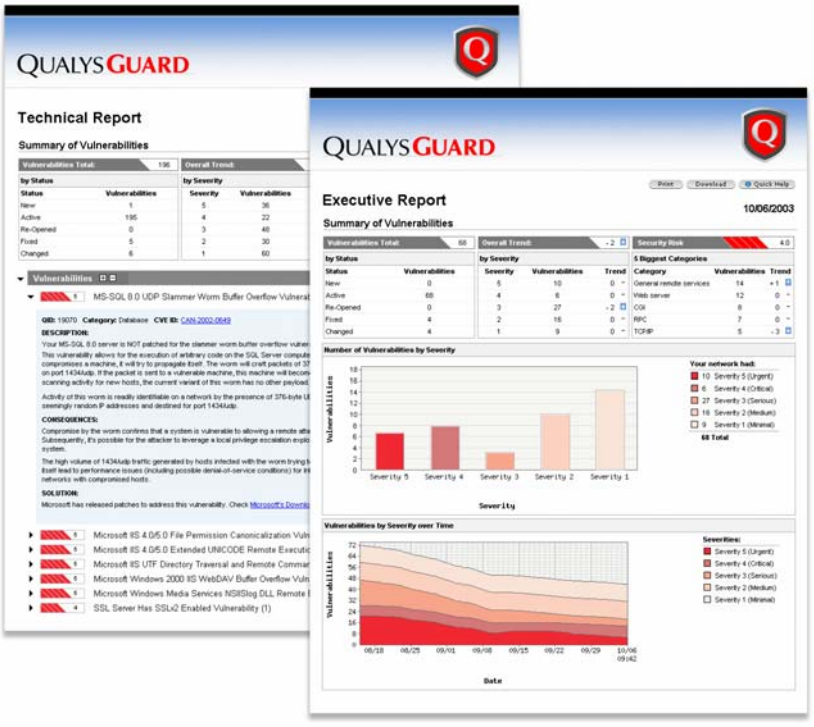

Figure 6—QualysGuard Vulnerability Report
By prioritizing vulnerabilities by severity, QualysGuard reports enable IT to deploy security resources where most needed.

© Qualys, Inc. All Rights Reserved

In addition, Qualys collects and publishes bulk statistical reporting data to help organizations identify common attacks and understand how their networks compare to those of other companies with a similar vulnerability profile. Management functionality for doing security audits, viewing reports and performing remedial activity can be distributed to appropriate security staffers throughout the enterprise. All information regarding specific enterprises is kept completely confidential.

QualysGuard's dynamic reporting extends to users the following benefits:

- Custom Reporting—users can create, run and save custom reports as templates.
- Vulnerability Trend Analysis—users can compare scan results over time, and from one scan to another.
- Graphical Reporting—users can view HTML graphical reports of discovered vulnerabilities and charts.
- Sorting and Filtering—users can sort and filter data from scanned results.
- Executive Summary Reporting—high-level reports can be produced with a global view of network security.

For companies that want to integrate QualysGuard information into third-party reporting tools, Qualys provides complete scan and map details in XML. QualysGuard reports can also be downloaded in HTML, MHT, and PDF.

Remedy: Links to Verified Fixes

For each vulnerability discovered, QualysGuard recommends verified countermeasures, patches, and workarounds, and provides links to Web sites providing documentation or patches. Security experts in Qualys' Vulnerability Laboratory test and validate remedies and provide time-to-fix estimates for vulnerabilities that can be resolved.

© Qualys, Inc. All Rights Reserved

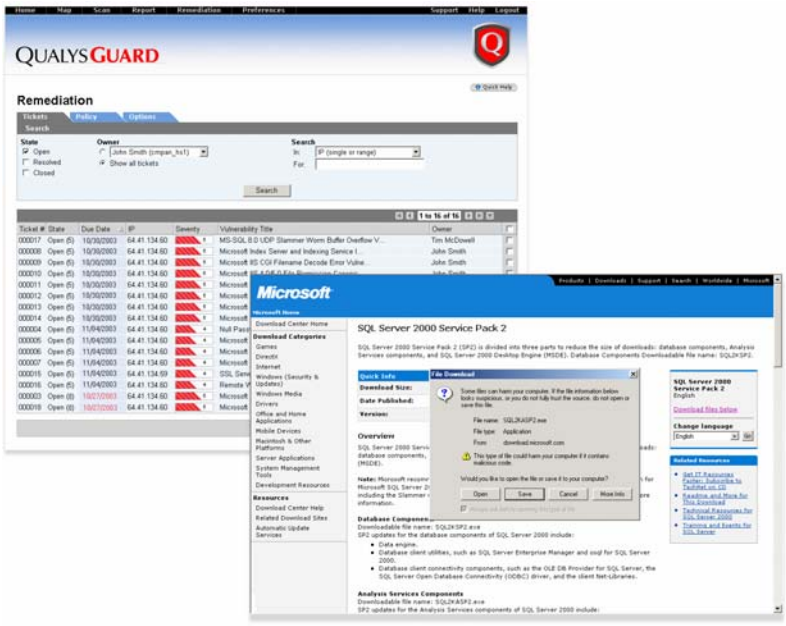

Figure 7—QualysGuard Links to Verified Remedies
Recommendations on immediate countermeasures, patches, and workarounds for each detected vulnerability, as well as time-to-fix estimates, are validated and provided by QualysGuard.

Some security auditing services typically notify administrators of vulnerabilities only if they know of available fixes, leaving administrators the difficult choice between remaining vulnerable to attack or shutting down vital information services. In contrast, QualysGuard reports all detected vulnerabilities, regardless of whether a patch is available. If a patch is not available, QualysGuard suggests workarounds that enable administrators to continue operating their networks while the vendors develop a fix.

Remediation Management

With the Remediation Workflow feature, network security managers can utilize QualysGuard as a workflow ticketing solution, automatically assigning repair activities to specified administrators. Individual users can then manage their assigned vulnerability remediation tickets. Ticket creation and ticket state/status adjustments occur automatically by the service, triggered by security audits and configured through policies. Tickets that have been resolved are immediately verified by QualysGuard and closed if successfully patched.

© Qualys, Inc. All Rights Reserved

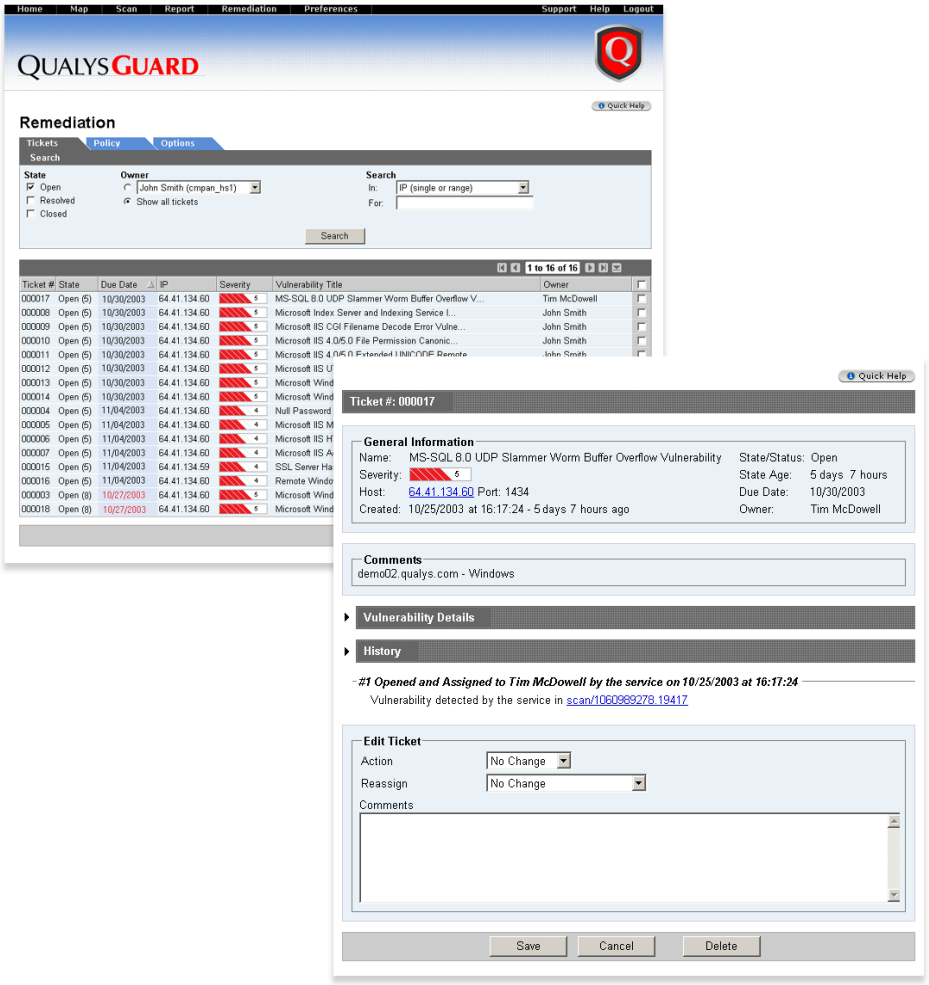

Figure 8—QualysGuard Provides Remediation Workflow
Network security managers can utilize QualysGuard as a workflow ticketing solution, automatically assigning repair activities to specified administrators for fast, accurate resolution.

Open API – Third Party Integration

The QualysGuard API allows third parties to integrate the QualysGuard automated solution into their own applications via an extensible XML interface. Qualys' open, XML-based API platform is unique in the security industry. The APIs programmatically expose core QualysGuard capabilities, including scan, map, scheduler, and preferences. This allows customers to customize their vulnerability assessment audits and integrate them tightly with their own security processes.

© Qualys, Inc. All Rights Reserved

On-Demand Security Audits are a Continuous Process

The on-demand security audit process is continuous: QualysGuard discovers, analyzes, and reports vulnerabilities, and companies apply the recommended remedies. Then users repeat the process to verify that the vulnerabilities have been eliminated. When companies first subscribe, they typically cycle through the process multiple times until few vulnerabilities remain, and none with high severity levels. Thereafter, scans are conducted at regular intervals and on-demand after a device or network setting has been changed.

© Qualys, Inc. All Rights Reserved

Conclusion

QualysGuard gives organizations a simple, effective, efficient, and affordable way to keep their networks secure. It provides subscribers with instant, real-time, on-demand access to network topology mapping, detailed reports about security vulnerabilities, and validated solutions.

Qualys, the pioneer in preventive online security auditing and a trusted vendor, is uniquely capable of helping customers ensure total security at the network perimeter and inside the corporate network. Through its non-intrusive, state-of-the-art scanning and advanced reporting techniques, Qualys helps customers secure their networks, comply with industry or governmental regulations pertaining to security and privacy, and achieve peace of mind.

For a Free Trial of the QualysGuard on-demand security audit service, please go to http://www.qualys.com/forms/?lsid=6468.

For a Free Scan, please go to https://freescan.qualys.com.

For a Guided Tour, please go to http://qualys.com/products/qgent/seetrybuy/guided/.

© Qualys, Inc. All Rights Reserved

Data Portability, APIs, and Third-Party Integrations

Qualys' open, XML-based API platform is unique in the security industry. The APIs programmatically expose core QualysGuard capabilities, including scan, map, scheduler, and preferences. This allows customers to customize their vulnerability assessment audits and integrate them tightly with their own security processes.

In addition to viewing reports using Qualys' Web-based interface, customers may manually or programmatically export their vulnerability data and scan results/reports in XML format using QualysGuard's open, published API specifications.

These capabilities are used in a number of current and in-process third-party integrations, including support for the leading firewall and intrusion detection system (IDS) providers. QualysGuard's firewall integrations continuously monitor firewall management consoles for vulnerabilities that may have been inadvertently introduced through firewall policy changes. QualysGuard's IDS integrations enable enterprises to automatically correlate ongoing attacks with actual target host vulnerabilities, reducing false alarms.

QualysGuard also integrates with vulnerability remediation systems to automatically push software patches, hot-fixes, configuration changes, and other remediation data to vulnerable machines.

For more information on the QualysGuard API, visit: http://www.qualys.com/docs/APIuser_10282003a.pdf

Appendix A: QualysGuard Web Services Architecture

The QualysGuard Web Services Architecture has several elements. The following diagram illustrates the QualysGuard Web Services Architecture and how the service communicates with customers' systems.

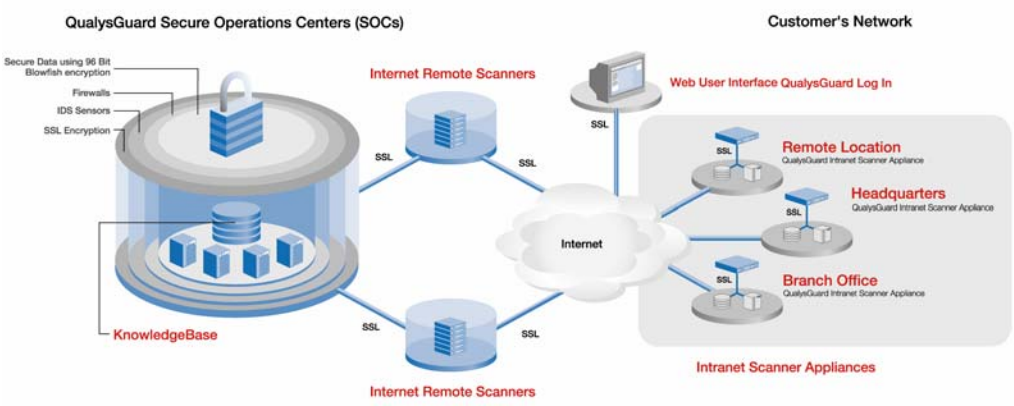

Figure 10—QualysGuard Web Services Architecture
QualysGuard architecture has six elements: – redundant Qualys Safe Datacenters, Qualys Security for Systems & Communications, dozens of QualysGuard Remote Scanners positioned throughout the world, QualysGuard Intranet Scanner Appliances, the QualysGuard KnowledgeBase and the QualysGuard Web User Interface.

QualysGuard Secure Operations Centers

QualysQuard Secure Operations Centers (SOCs) offer secure storage and processing of vulnerability data on an n-tiered architecture of load-balanced application servers. Redundant SOCs include a primary operations center in Santa Clara, Calif. The operations center is hosted at a secure Cable & Wireless datacenter, including redundant systems and network access. All computers and racked equipment are isolated from other systems in a locked private vault. Access is restricted to Qualys operations employees using ID badge and biometric authentication. Qualified Qualys security engineers monitor operations 24x7x365. As part of the hiring process, all employees undergo third-party reference and background checks, and sign confidentiality agreements.

Qualys Security for Systems & Communications

Security of Qualys Secure Operations Centers is documented in a successful SAS-70 audit of Qualys data storage access methods and

© Qualys, Inc. All Rights Reserved

controls. An audit by @stake also documents a successful Qualys security architecture review and penetration test. Systems are configured with a host-based "multi-homed" firewall, a policy-driven file system, an integrity checking system, and intrusion detection system. QualysGuard servers connect to the report database via private (non-routable) IP addresses. Logged access requires use of two-factor authentication technology. VeriSign, Inc. provides digital certificates and an internal ticketing system to guarantee timely renewal of certificates. Operations are redundant and load balanced for optimum system performance.

QualysGuard uses HTTPS (SSLv3) and strong cryptography for all communications with users. No clear text communications are supported for any aspect of QualysGuard, including navigation of user interface, launching scans or running reports. QualysGuard uses SSH (Secure Shell) software for login by Windows or Unix clients, replacing insecure options such as telnet and FTP. Qualys will integrate support for two-factor authentication using SecurID and client certificate support in Q4'2003.

No user passwords are stored on QualysGuard servers, nor does Qualys have access to any user password. The KnowledgeBase contains the MD5 hash of the user's password, which is created during account setup and is used for authentication. If a user forgets the QualysGuard password, it cannot be recovered so access is lost forever to prior customer vulnerability audit data. Customer data is encrypted with Blowfish-CBC without IV. The vulnerability report key is randomly generated per customer account. QualysGuard never writes this key to disk in clear text or stores it anywhere other than in memory. Audit data is encrypted and stored on a per-customer basis so no one—even a Qualys administrator with full system privileges—can read customer audit data.

QualysGuard Internet Remote Scanners

Internet Remote Scanners provide the fastest, most efficient perimeter scanning available with more than five-dozen scanners placed in key global locations. Internet Remote Scanners underpin a distributed, inference-based scanning mechanism that speeds security audit data gathering and processing. The architecture supports three elements:

- Intelligence gathering
- Automated, non-destructive test mechanisms for intelligent scans coupled with a detailed KnowledgeBase
- Audit processing and evaluation process that emulates security experts

Remote Scanners are a collection of scriptable modules that implement scanning as a multithreaded process on QualysGuard's n-tiered architecture of load-balanced application servers. In this manner, QualysGuard scans and processes security audits in parallel for optimum speed of operations. Inference-based scanning in QualysGuard is an "expert systems" approach that learns information about a system in exactly the same fashion that a hacker would. With inference-based

© Qualys, Inc. All Rights Reserved

assessment, Remote Scanners begin by building an inventory of protocols found on the machine undergoing an audit. After the protocols are discovered, the scan proceeds to detect which ports are attached to services, such as web servers, databases, or e-mail servers. After determining the set of services present on a machine, inference-based vulnerability assessment then selects vulnerabilities that could be present based on each machine's exact configuration, and executes only those relevant tests.

Scanners use active OS discovery techniques such as banner grabbing and binary grabbing, OS specific protocols, and TCP/IP stack fingerprinting, and passive techniques such as packet spoofing. Fingerprinting entails careful inspection for subtle variations in implementation of RFC standards. A service discovery engine detects backdoors, Trojans and worms by checking more than 120 TCP and UDP services, including those on non-default ports and with fake banners. A similar discovery process is used to fingerprint HTTP applications, including version ID, service pack ID, and installed patches. QualysGuard correlates OS and HTTP fingerprint tests to quickly find true vulnerabilities and minimize false positives.

QualysGuard Intranet Scanner Appliances

The Intranet Scanner is a client-side plug-in appliance used for gathering security audit data inside the firewall and for secure communications with QualysGuard Remote Scanners. Intranet Scanner uses a specifically hardened operating system kernel designed to prevent shell-code and buffer overflow attacks. It contains no services or daemons exposed to the network. Setup requires just a few minutes using an LCD panel and keypad to enter user name, IP address, DNS and proxy data. The appliance is virtually managed by Qualys over the web. Communications use strong encryption and SSLv3 via port 443. The appliance polls QualysGuard to automatically to download software updates and new vulnerability signatures, and to process job requests for network discovery and scanning. Intranet Scanner does not retain scan results; instead, all data is securely encrypted, transmitted, and stored at redundant Qualys operations centers.

QualysGuard KnowledgeBase

The KnowledgeBase is the crown jewel of QualysGuard architecture. It contains the intelligence fueling comprehensive on-demand network security audits, vulnerability management, and remediation. Qualys updates the KnowledgeBase daily with signatures for new vulnerabilities, validated patches, fixes for false positives, and other data to improve the effectiveness of its security audit web service. The KnowledgeBase has

© Qualys, Inc. All Rights Reserved

signatures for thousands of vulnerabilities and has the most extensive database in the security industry – thereby, detecting more vulnerabilities, and more “important” vulnerabilities than any other vendor. Qualys’ vulnerability audit database is fully published and CVE compliant.

All QualysGuard subscribers automatically reap benefits from new updates to KnowledgeBase because Qualys Remote Scanners and Intranet Scanners always use the newest version of KnowledgeBase. Users of the QualysGuard web service are thus always testing for the latest vulnerabilities.

QualysGuard Web User Interface

The Web User Interface makes the QualysGuard web service easy to use. Any standard web browser lets you navigate the QualysGuard user interface, launch scans, and examine audit report data. Communications security is provided via HTTPS (SSLv3) encryption. QualysGuard uses SSH (Secure Shell) software for login by Windows or Unix clients, replacing insecure options such as telnet and FTP. Qualys will integrate support for two-factor authentication using SecurID and client certificate support in Q4’2003. With a web browser, users control the four-step process of the QualysGuard web service:

- Discover – dynamic identification of network devices
- Audit – automatic assessment of security exposure
- Report – actionable reporting with trend analysis
- Remedy – tracking vulnerabilities and applying patches

© Qualys, Inc. All Rights Reserved

Appendix B: Glossary

DHCP The Dynamic Host Configuration Protocol, a communications protocol that lets network administrators centrally manage and automate the assignment of Internet Protocol (IP) addresses in an organization's network.

Exploit An attack on a network vulnerability that potentially results in compromising network security.

Exhaustive Search An algorithm that finds a solution to a problem by trying every possibility.

Fully Qualified Domain Name A fully qualified domain name (FQDN) is that portion of an Internet Uniform Resource Locator (URL) that fully identifies the server program to which an Internet request is addressed. The FQDN includes the second-level domain name (such as "mycompany.com") and any other levels (for example, "www.mycompany.com" or "www1.mycompany.com").

IP The Internet Protocol (IP) is the method or protocol by which data is sent from one computer to another on the Internet. Each computer (sometimes known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet.

IP Address In the most widely installed version of the Internet Protocol (IP) today—that is, version 4 — an IP address is a 32-bit number that identifies each sender or receiver of information that is sent in packets across the Internet. An IP address is usually expressed as four decimal numbers, each representing eight bits, and separated by periods (for example, 210.29.32.112). Each IP address has two parts: the identifier of a particular network on the Internet and an identifier of the particular device (which can be a server, workstation, or other device) within that network (the "local" part). On the Internet itself—that is, between the router that move packets from one point to another along the route—only the network part of the address is noted. For Class A IP addresses, the local and network numbers represent an IP address of the form "network.local.local.local." For a Class C IP address, they represent an address of the form "network.network.network.local." The number version of the IP address can (and usually is) represented by a name or series of names called the fully qualified domain name.

Internet Remote Scanner A software tool that facilitates fast, efficient external (perimeter) scanning. Internet Remote Scanners are enabled on Qualys servers in Qualys Secure Operations Centers. Its inference-based scanning engine ensures highly accurate vulnerability detection and elimination of false-positives.

© Qualys, Inc. All Rights Reserved

Intranet Scanner Appliance Appliance version of Internet Scanner that enables internal network auditing. Fully automated with the latest vulnerability signatures. Employs secure communications with SSL layer.

Intrusion Detection Network security assessment “from the inside” via software or hardware tools that examine either low level network packet data (“network-based intrusion detection”) or operating or file system calls (“host-based intrusion detection”) for inappropriate data patterns or other unauthorized activities.

Network Security Assessment The evaluation of the security of an organization’s network to attacks that originate either inside or outside the organization.

Network Vulnerability A weakness in a computer, network device, software application, or other component that enables it to be used for purposes other than those intended.

Port Number In TCP/IP-based networks, an end point to a logical connection between two IP addressable devices. A port number often identifies the particular TCP-based service running at the connection. For example, port 80 is typically used for HTTP traffic.

TCP Because IP is a connectionless protocol, there is no continuing connection between the end points that are communicating, and each packet that travels through the Internet is treated as an independent unit of data without any relation to any other unit of data. Transmission Control Protocol transmits the packets in the right sequence in Internet communications.

Vulnerability Assessment Network security assessment via intentional attempts to identify weaknesses using the controlled application of known attacks.

Vulnerability Management Incorporates a combination of processes and technologies which includes asset discovery, vulnerability assessment, analysis of audit results, and the management of corrective actions/remediation.

Vulnerability Scanner A software tool that initiates the discovery of a targeted network’s vulnerabilities.

© Qualys, Inc. All Rights Reserved

About Qualys

Qualys, Inc. is the market-leading Web Service Provider offering on-demand network security audits and vulnerability management. The Qualys flagship service, QualysGuard, is delivered through a global Web service architecture and performs more millions of scans per quarter on networks owned by thousands of organizations, including ABN Amro, Hershey Foods, Hewlett Packard and The Thomson Corporation.

Customers rely on QualysGuard for reliable protection against worms and hackers while providing trusted third-party certification of network security. More than 150 Fortune 1000 companies, federal and state agencies, and hundreds of small to medium businesses use the QualysGuard Web service to measure and enforce network security effectiveness, reduce risk and comply with government regulations.

Founded in 1999, Qualys is a private company with 50 million in funding from Trident Capital, ABS Ventures, Mercury Interactive, and VeriSign. Qualys is headquartered in Redwood Shores, California, with global offices in France, Germany, U.K. and the Pacific Rim.

Qualys, Inc.
1600 Bridge Parkway
Redwood Shores, CA 94065
T: (650) 801 6100
F: (650) 801 6101

For more information, visit www.qualys.com

Qualys Document ID: 121503WP

© Qualys, Inc. All Rights Reserved