Strengthening Network Security With Web-Based Vulnerability Assessment

EXECUTIVE SUMMARY

The need to beef up network security usually gets the best of intentions. Frequent stories of successful hackers and cyber-criminals convince us that something must be done to better protect critical digital assets. But many take action only after trouble hits their own network. Prudent organizations are using protective measures with one or more of the standard network security technologies—virus detection, firewalls and intrusion detection systems (IDS). These tools are essential elements for network security. Unfortunately, even these are vulnerable to attack when improperly configured or not updated for the ever-changing nature of sophisticated new, automated threats from hackers and cyber criminals. For example, even organizations that deployed these security technologies were vulnerable to Code Red and Nimda worms, which penetrated through these systems.

The emerging Fourth Pillar of network security is vulnerability assessment (VA). It complements the other three technologies by automatically detecting network security holes and advising security specialists how to fix them—fast. Code Red and Nimda damage could have been avoided with VA, since it protects networks from known vulnerabilities. A Web-based service such as QualysGuard from Qualys, Inc. boosts the effectiveness of security infrastructure. It speeds proactive remedies with vulnerability rankings that prioritize repair efforts and provide one-click links to verified remedies. The result is a complete security measurement system that dramatically frees up staff time by automating vulnerability assessments from any Web browser. VA also can shrink the operation costs for security audits and repairs by up to 90%.

This guide describes a new breed of digital security challenges, explores how vulnerability assessment boosts the effectiveness of traditional security technologies, and details the service benefits of QualysGuard, the first scalable, automated, Web-based solution that is cost-effective for organizations of all sizes. It concludes with offering a Free 7-Day Trial of QualysGuard.

THE REAL NEED FOR DIGITAL SECURITY

"Vulnerability Assessment is a critical element of network security. Frequent use of an automated, Web-based VA service such as QualysGuard helps companies to consistently improve and verify the protection of their digital assets cost-effectively."

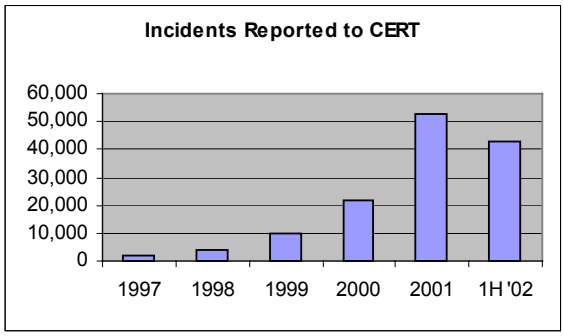
Allan Carey
International Data Corp.

Malicious breaches can funnel trade secrets to unscrupulous competitors, trigger direct financial losses, and quickly cripple the trust of customers, partners and employees. Swift negative reactions by insurers and financial markets could be fatal to a company.

The risks of digital mischief by hackers and disgruntled employees are widely known. Many organizations have responded by implementing digital security measures such as virus detection, firewalls and IDS. Yet despite these steps, reports of IT security incidents and related damage are rising geometrically.

Digital Crime Incidents are Rising Geometrically

One top-line snapshot is from the CERT Coordination Center at Carnegie Mellon University, the U.S. government-funded clearinghouse for cyber infractions, vulnerabilities, alerts and patches. Total incidents reported have grown 2,368% from 1997 to 2001—an annual average compound rate of 474%. Incidents reported through the first half of 2002 are 82% of the total reported for all of 2001 (see www.cert.org/stats/cert_stats.html).



Financial losses due to computer breaches also are rising dramatically as evidenced by statistics from the annual CSI/FBI Computer Crime and Security Survey (see www.gocsi.com). Such losses were reported by 80% of 503 mostly large U.S. organizations responding to the 2002 survey. The 223 that could quantify losses disclosed total damage of $455,848,000 in 200—an average loss of more than $2 million. The average compound growth rate of these losses disclosed since 1998 is 47%.

Fallout From Security Breaches Affects Many People

The geometric rise in security breaches reflects more than careless joy hacking by solo pranksters. The reported deliberate criminal acts of online theft and disruption affect hundreds of thousands, if not millions, of people. Consider these recent news events:

- Hackers broke into the State of California personnel database in April 2002 and gained access to financial information for all 265,000 state workers, including names, Social Security numbers and payroll data (*San Francisco Chronicle*, 5/25/02).
- About 13,000 customer records-work and home addresses, Social Security and account numbers, and credit histories-were stolen over a 10-month period from Experian Information Solutions through Ford Motor Credit Co. (*New York Times,* 5/17/02).
- Hackers breached the firewall-protected Playboy.com Web site and accessed customer credit card numbers in November 2001 (*CNN*, 11/20/01).
- A "security researcher" breached a *New York Times* database holding Social Security numbers, home telephone numbers and other personal information of 3,000 employees and article contributors such as Jimmy Carter, Rush Limbaugh and

Robert Redford (*InformationWeek*, 2/27/02).

- The "Code Red" and "Nimda" worms last year tied up Internet traffic and caused more than $3 billion in damages and economic disruption worldwide, according to a study by research firm Computer Economics (*ABC News*, 1/22/02).

Meeting Requirements for Digital Security

Businesses have a clear economic incentive to thwart digital intrusion. Some organizations also must comply with regulatory statutes aimed at bolstering security. For example, financial institutions must follow security guidelines in the Gramm-Leach-Bliley Financial Services Modernization Act (GLBA). Health insurers have similar requirements in the Health Insurance Portability and Accountability Act (HIPAA). Corresponding regulations exist in other countries. Property and casualty insurance companies also are demanding that customers implement more rigorous, audited security procedures.

Apart from these issues, another motivation for hardening security is the specter of cyber-attacks by terrorists such as al Qaeda and hostile nation states. Experts cite rising evidence of systematic probes over the Internet to vital infrastructure such as nuclear power plants, gas facilities, electrical generation and transmission, water storage and distribution, and emergency telephone systems (see *Washington Post*, 6/27/02). Some fear unauthorized seizure and remote control of devices managing vital services.

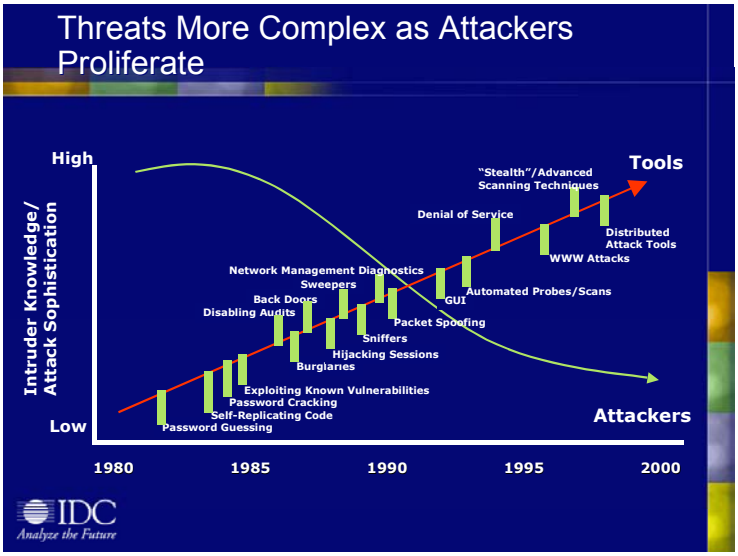
The good news is that, properly implemented, network security technology and procedures can thwart virtually all attacks through the Internet, whether by independent hackers, organized criminals, or terrorists. Most attacks exploit known security weaknesses. Security managers can prevent most attacks if they take proper steps to secure networks. Installing traditional security tools such as anti-virus, firewall, and IDS is a good start. But to maximize proactive effectiveness of these security subsystems, organizations require frequent, systematic assessments of performance against vulnerabilities within the network system.

WEB-BASED VULNERABILITY ASSESSMENT BOOSTS EFFECTIVENESS OF SECURITY TECHNOLOGIES

"A continuous Vulnerability Assessment Web service like QualysGuard can provide rapid indication of changes in configuration that have resulted in security vulnerabilities."

John Pescatore
Gartner Research

A vulnerability assessment tests network security infrastructure and systems for known attack weaknesses. It systematically maps all IP connections, tests and analyzes the repellant capabilities of these resources against known security holes, and provides verified remedies. Manual assessments by security staff or outside consultants, unfortunately, are labor intensive and usually outdated before completion. The slow pace of a manual assessment leaves networks vulnerable to new attack technology, which changes daily. The top attack trends noted earlier by CERT are automation and increasing sophistication of attack tools. The frequency, complexity and rapid change of new attacks makes regular vulnerability assessments a requirement for effective security. Casual or non-technical intruders can inflict huge damage now, thanks to automated attack technology, a relationship shown in the following diagram.



Source: International Data Corporation

Fighting Back With Automated Vulnerability Assessments

Since automated attack tools make hackers and criminals more effective, security managers need to fight fire with fire by automating defensive measures. First on the list is automating traditional time-consuming, labor-intensive vulnerability assessments.

A major challenge for security managers is quickly understanding and prioritizing all active risks to network security—prerequisites for proactively fortifying the defensive infrastructure. Frequent vulnerability assessments of the repellent capabilities of firewalls and IDS are the only way to proactively ensure complete network security. And time is of the essence, because weaknesses must be fixed immediately. Otherwise, security managers are playing a dangerous game of chicken in which the odds are stacked toward malicious penetration. The automated capabilities of Web-based vulnerability assessment speed the processes of measuring security quality and managing related repairs.

QualysGuard is a Web-based vulnerability assessment service that takes the hacker's point of view by automatically but non-intrusively testing IP-based security infrastructure against all known vulnerabilities—including daily updates from CERT, network hardware manufacturers, software providers and other sources.

- QualysGuard is a self-contained Web-based service. Users do not need any new hardware, software, staff, or special training to get the benefits.
- Subscribers of QualysGuard are entitled to unlimited network assessments 24x7, including automated scheduling capability.
- With QualysGuard, security specialists can view scan results from any Web browser, link to remedial recommendations, and download patches and fixes—all with the click of a mouse.
- QualysGuard automatically inventories and fingerprints every IP device on the network. It creates a visual map for spotting unauthorized hardware, poor system configurations, and other potential attack points.
- QualysGuard provides automatic analysis of security quality for all network system elements. The service rapidly delivers results in an email report that ranks and prioritizes vulnerabilities by severity.
- To assist with complete vulnerability management, QualysGuard also provides tested remedies, where they exist, from software vendors to resolve exposures, or workarounds as well as time-to-fix estimates.

> *"Online scanning services such as QualysGuard turn the Internet itself into a tool against would-be network intruders."*
>
> **Craig R. Torgerson**
> **VP and Technology Manager**
> **Bremer Financial**

As the Fourth Pillar of network security, vulnerability assessment is an essential part of every organization's security infrastructure. Results from QualysGuard's solution leverage security staff efforts to fortify network administrators' effectiveness at thwarting attacks and freeing security specialists to focus on other tasks. The other three pillar—virus detection, firewalls and IDS—cannot collectively prevent penetration from intruders without regular vulnerability assessments. QualysGuard's Web-based service eliminates the constant worry of overlooking new vulnerabilities, automatically alerting network administrators when, where and how to install new patches or change security configurations. It provides one-click solutions for security holes and helps network administrators get their money's worth from existing security infrastructure, strengthening defenses against known attack technologies and techniques.

QUALYSGUARD BENEFITS: COST EFFECTIVE, RAPID HARDENING OF NETWORK SECURITY

1 Increase value of virus detection, firewalls, and intrusion detection systems by automating discovery of weak spots in security configurations

Digital security technology is the first line of defense against intruders. Strong protection requires the Four Pillars of security: virus detection, firewalls, IDS and vulnerability assessment (VA). The onslaught of new, changing threats makes VA essential for proper configuration and tuning of security infrastructure. Each QualysGuard scan produces a full inventory and graphical map of all IP devices, and discovers known security vulnerabilities in the network system. The complementary role of VA boosts the value of security infrastructure by advising security professionals when and how to proactively tune element configurations for maximum ongoing protection.

"Qualys has created a Managed Vulnerability Assessment platform to help companies like ours anchor their security policies with an automated, scalable and proactive solution that will result in a bottom-line return on investment."

Deefay Young
Senior Network Security Analyst
Adobe Systems

2 Speed vulnerability repairs, achieving more efficient security staff deployment, by ranking and prioritizing vulnerabilities and linking to validated remedies

Time is of the essence to ensure maximum protection. Digital attack sophistication is rising with the number of constantly probing marauders. Security administrators have no time to spare because new vulnerability warnings and security alerts appear daily. VA eliminates the constant worry of overlooking a new vulnerability. It also ranks the severity of problems to help prioritize repair actions. Using a vulnerability assessment service is like having an in-house, professional digital security research team correlating known configuration and patch requirements with your unique infrastructure, 24x7.

"QualysGuard eliminates the need to hire experts on each of our operating systems and applications. The type of knowledge and recommendations that Qualys offers is invaluable."

Lenard East
VP Network Engineering and Operations
Bank of the West

3 Provide dramatic operational cost savings for assessment and patch management while automatically finding newest threats

There are three options for vulnerability assessment: (1) manual testing with software-based products, (2) using consultants for penetration testing, or (3) Web-based vulnerability assessment. Using manually operated tool sets is labor intensive and expensive. Manually scanning one server easily requires one or two hours of a security specialist's time—for each scan. Just two scans a month for a company with 100 servers would boost the resource burden up to 400 hours a month, or two full-time people. Each scan of one custom server could take 10-20 hours. Hiring consultants to conduct penetration testing incurs even higher expenses. Customers with environments similar to this example who use a Web-based VA solution like QualysGuard dramatically reduce these

operational costs. These customers typically require just 20% of one person's time to review reports and implement recommended fixes—a 90% reduction in operating costs. QualysGuard also provides complete flexibility by permitting unlimited audit scans. QualysGuard reports always include analysis with the most up-to-date vulnerabilities. They provide one-click access to patches and solutions for implementation by your security team.

"Our staff is simply too busy to spend hours each day trying to monitor every security vulnerability. QualysGuard gives us a quick way to prioritize what we need to work on first. We use it as a second pair of eyes – to make sure that we have all the right patches installed and that we haven't missed anything during server or firewall reconfigurations."

David Mortman
Senior Manager of Information Technology
Siebel Systems

Reduce human error by double-checking actions of security staff with unbiased, reliable auditing

Even the best of us makes an occasional mistake. QualysGuard helps avert security-related mistakes by serving as an extra pair of eyes that never sleep. Running audits before and after installing new gear or software can ensure proper configuration of security infrastructure parameters. One example is QualysGuard's ability to continuously and automatically monitor firewalls for vulnerabilities that may have been inadvertently introduced by policy changes. QualysGuard makes security staff efforts more objective because it simulates a hacker's perspective while probing for vulnerabilities through the network.

5 Scale by handling IP networks of any size

QualysGuard is not bound by special network, security or other IT infrastructure. The Web-based service instantly scales to any-sized IP network simply by entering the range of IP addresses desired for an audit. The service even handles Class C and B size networks with ease. QualysGuard effectively audits the security of rapid major additions to an IP network, such as acquiring or merging with another corporation.

"Assessing your own network's security is like trying to proofread your own report. It's clearly more effective to outsource vulnerability assessment to an outside, disinterested party."

Kevin Ertell
Director of Online Operations
Tower Records

6 Simplify setup and operations with no changes to network, no client software, no gurus

Traditional management of network security infrastructure is complex. Using Web-based VA is simple, and knowledge gained with VA simplifies managing the security infrastructure. Security audit scans require no special hardware or software. Any standard browser allows administrators to run scans, view findings and download patches. VA uses the industry standard TCP/IP for communications with security infrastructure so it requires no special configuration—or security gurus—to perform audit scans. No training is required. Operators simply enter a range of IP addresses into a Web form requesting the scan and click the "start" button. Everything else is automatic.

7 Get 24x7 unlimited auditing and near-instant online reports

QualysGuard is always available to assess the safeguarding of network-accessible digital assets. Automatic audit scans may be pre-scheduled or performed on demand as often as security administrators like. Detailed reports, security configuration advice, and hotlinks to patches and problem fixes appear via email shortly after completing a network audit. Extensive trend analysis is also available for network mapping and vulnerabilities.

HOW QUALYSGUARD WORKS

> *"Qualys has provided Fujitsu with a distributed, scalable global architecture on which to base our new remote auditing service. This is an unprecedented weapon in the battle against network intruders and emerging network vulnerabilities, enabling customers to take a truly proactive stance against attack."*
>
> **Hiroaki Kurokawa**
> **Group President**
> **Fujitsu**

QualysGuard's solution allows customers to initiate unlimited scans, either pre-scheduled or on demand, from any Web browser. Subscription pricing is based on the number of IP addresses scanned. Security professionals can run as many scans as necessary whenever needed to identify vulnerabilities, access tested remedies, and confirm that remedies were successful.

As a managed service, QualysGuard requires no installation, set-up, hardware or software purchases or maintenance, in-house security expertise, or special training. It provides unlimited scans, allowing network administrators to reassess vulnerabilities every time they add, remove or change a device. QualysGuard is a continuous VA service. As shown in the figure below, customers get all service components, including (1) discovery of all networked IP devices, (2) analysis against the most recent vulnerabilities, (3) browser-accessed summary and detailed reports, plus (4) remedies and workarounds.

FREE, EASY TRIAL

Experience the benefits of Web-based vulnerability assessment with a Free 7-Day Trial of QualysGuard. Here are the easy steps:

- Complete a short form at https://www.qualys.com/forms/main_trial.php or call a Qualys sales representative at **1.800.745.4355**.
- Qualys will assign an account name and password for the free trial.
- Use your login and password to launch your trial.
- View the scan's results, read suggested solutions, download patches and fix security problems.
- Repeat scans as often as you like for seven days.

ABOUT QUALYS, INC.

Qualys, Inc., the leader in Web-based vulnerability assessment, enables security providers, security professionals, and corporate customers to automatically audit Internet-connected networks for security vulnerabilities. Qualys' innovative Web service delivers automated, scalable, and cost-effective security auditing and risk assessment of global networks, inside and outside the firewall. Founded in 1999 by a team of Internet security experts, Qualys is headquartered in Redwood Shores, California, with offices in France, Germany and the U.K. Enterprises of all sizes, from Global 2000 companies to small business, rely upon the QualysGuard service as their first line of network defense, including: Adobe Systems, Agilent Technologies, Apple Computer, Bank of the West, BlueCross BlueShield, BT Ignite, Fujitsu, Hewlett Packard, the Royal Bank of Scotland, Siebel Systems, TIAA-Cref, and Tower Records.

Securing Your Network

Qualys, Inc.
1600 Bridge Parkway
Redwood Shores, CA 94065
800.745.4355
www.qualys.com