Guide to Effective Remediation of Network Vulnerabilities

Steps to Vulnerability Management are Prerequisites for Proactive Protection of Business System Security

Vulnerability Management

Identifies all known risks

Minimizes false positives

Fixes vulnerabilities fast

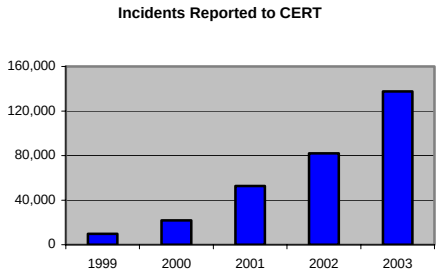
EXECUTIVE SUMMARY

Remediation of network vulnerabilities is something every organization wants done *before* hackers exploit the weaknesses. Effective remediation entails continuous processes that together are called Vulnerability Management. The processes and related technology defined by vulnerability management help organizations efficiently find and fix network security vulnerabilities. Systematic use of these processes protects business systems from ever more frequent viruses, worms and other network-borne attacks.

Continuous Processes of Vulnerability Management

- Create security policies & controls
- Track inventory / categorize assets
- Scan systems for vulnerabilities
- Compare vulnerabilities against inventory
- Classify risks
- Pre-test patches
- Apply patches
- Re-scan and confirm fixes

These steps used to be manual and cumbersome. You can automate most of them now with security applications and Web-based services, such as QualysGuard. For maximum effectiveness, all steps of the vulnerability management cycle must be done with consistent, timely execution. Focusing on just one of the processes, such as patching, is like plugging one hole in the dike. Automation with QualysGuard provides on demand vulnerability management. Automation is also a cost effective way for organizations to minimize security risks to business applications. An important byproduct of vulnerability management is documented compliance with laws and regulations for security, personal privacy and corporate governance.



URGENT NEED FOR VULNERABILITY MANAGEMENT

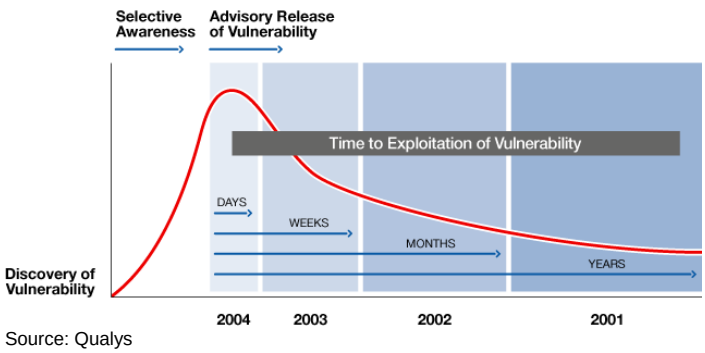
Rising volume, widespread exposure and acceleration of successful attacks underscore the urgent need for vulnerability management. The CERT Coordination Center at Carnegie Mellon University says the volume of security incidents reported has grown 1,295% from 1999 to 2003—an annual average compounded rate of 69.4% (www.cert.org/stats/cert_stats.html).

Organizations are more exposed to network vulnerabilities. New research from Qualys analyzing more than 1.9 million network vulnerabilities during a recent 24-month period shows why. The data were a statistically valid sample anonymously drawn from three million security scans with QualysGuard made by Global 2000 organizations. Analysis revealed four Laws of Vulnerabilities:

- **HALF-LIFE** – The half-life of critical vulnerabilities is 30 days and doubles with lowering degrees of severity
- **PREVALENCE** – Half of the most prevalent and critical vulnerabilities are being replaced by new vulnerabilities each year
- **PERSISTENCE** – The lifespan of some vulnerabilities is unlimited; old risks recur partly due to new deployment of PCs and servers with faulty unpatched images of hard drives
- **EXPLOITATION** – 80% of vulnerability exploits are available within 60 days after news announcements of vulnerabilities

Attacks have dramatically accelerated damage by using sophisticated technology for automatic replication, pre-identification of vulnerable hosts, and targeting specific classes of intended victims. Recent attacks with blended worms triggered global damage just in a few minutes. No one had time to react with protective measures. Automated attacks with active worms require no human interaction, so they can ensure more damage than the first generation of generic viruses. Recent examples were Slapper (9/02), SQL Slammer (1/03), Blaster (8/03), Witty (3/04) and Sasser (5/04). SQL Slammer globally infected more than 90 percent of 75,000 hosts running Microsoft SQL Server within 10 minutes. Blaster infected more than 100,000 systems per hour at its peak taking advantage of the most prevalent vulnerability in the world.

These threats are also emerging faster than ever. In the past, the discovery/attack lifecycle was a year or more from the advent of discovering a vulnerability to widespread exploitation. SQL Slammer happened six months after discovery, Slapper was six weeks, Blaster and Nachi were three weeks, and Sasser two and a half weeks after. Witty was the fastest worm, striking just one day after vulnerability was announced. It compromised 12,000 vulnerable hosts within 45 minutes. In cases like Witty, the attack is over before you can patch the vulnerability. Vulnerability management provides the only means to cut the odds of a successful attack and protect business system security.



Source: Qualys

"The Qualys on demand platform allows us to audit our security status at any moment and manage network vulnerabilities on a centralized enterprise-wide level with a fraction of the resources and cost."

Mark Iovinelli
Enterprise Design & Implementation Team Manager
RR Donnelley

VULNERABILITY MANAGEMENT PRIMER

Vulnerability management entails continuous processes combined with labor saving technology to help organizations effectively find and fix network security vulnerabilities. Organizations can automate many vulnerability management processes. Automation improves accuracy and speeds remediation to ensure better protection for critical business systems. The table below summarizes requirements and solutions each process of vulnerability management.

Processes of Vulnerability Management

Process	Requirements	Solution
Create security policies & controls	Define these to guide security efforts, for the entire organization down to configurations for security devices, servers, network services, applications and endpoint PCs.	Mostly manual; some automation possible on desk tops
Track inventory / categorize assets	Vulnerabilities must be found before they can be patched. An inventory of IP devices, services and configurations allows correlation with known vulnerabilities for faster, accurate remediation. Categorize assets to prioritize remediation.	Automate with QualysGuard
Scan systems for vulnerabilities	Do regular or continuous scans of all IP devices attached to the network. Use industry standard vulnerability lists such as CVE, CERT, SANS20 and other private sources. Software-based solutions require maintenance and updates. An on demand service like QualysGuard automatically scans for up-to-date vulnerabilities.	Automate with QualysGuard
Compare vulnerabilities against inventory	Identifies actual vulnerabilities in the network. Minimizes false positives by matching known vulnerabilities against actual configurations of devices, services and applications.	Automate with QualysGuard
Classify risks	Rank each actual vulnerability from most serious to least serious. This prioritizes what to fix first.	Automate with QualysGuard
Pre-test the patch or other remediation	Obtain the correct patch to fix the identified vulnerability. Test in your environment to ensure the patch corrects the vulnerability without affecting technology or business operations.	QualysGuard and manual testing
Apply the patch	Use a patch automation system that provides rollback capability in case you have to uninstall the patch.	Automate with software from Qualys partners
Re-scan and confirm the fix	Rescan to ensure the vulnerability was fixed by application of the patch.	Automate with QualysGuard

Source: Qualys

Vulnerability Management Improves Security

Organizations do vulnerability management to:

1. Fix faults in the software affecting security, performance or functionality.
2. Alter functionality or to address a new security threat, such as by updating an antivirus signature.
3. Change a software configuration to make it less susceptible to attack, run faster or improve functionality.
4. Use most effective means to thwart attacks by automated worms.

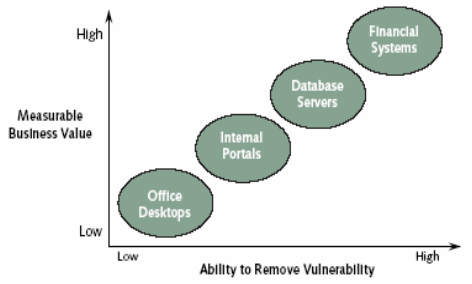
"Qualys' on demand model is like turning on a light – immediate visibility into ranked vulnerabilities and the fastest path to remediation, preventing attacks before they occur."

Robert S. Paszko
Director of Security
DuPont

Most remediation efforts are for fixing mistakes in software. As much as we rue their presence, there are five to twenty bugs in every thousand lines of software code, according to the National Institute of Standards and Technology (http://csrc.nist.gov/publications/nistpubs/800-40/sp800-40.pdf, p. 1). It's a problem that will not vanish in the foreseeable future so dealing with it is the only practical option. Systematic use of vulnerability management processes is the best possible means for strong network security. It helps keep organizations out of reactive mode and safe from attacks. The rest of this section shows how to do vulnerability management smarter, better, faster, and for lower overhead.

Create security policies and controls to know how to respond

Policy management is critical. Enterprise policies start at the top of an organization and require executive oversight. Policies determine the nature of controls used to ensure security, such as standard configurations for all security devices and applications including antivirus, firewall and intrusion prevention. Policies and controls also should include servers, network services, applications and endpoint PCs. In the past, policy management was a manual, cumbersome process. New software tools can automate some aspects of policy management and enforce configurations on endpoint devices. Automation saves time, improves accuracy and lowers total cost of ownership.



Categorize assets by business value to prioritize vulnerability remediation

Track Inventory / Categorize Assets

You need to find vulnerabilities before you can fix them. This step sets an evaluation baseline by creating and maintaining a current database of all IP devices attached to the network. Organizations should categorize assets by business value to prioritize vulnerability remediation. Elements in the database include all hardware, software, applications, services and configurations. Tracking this level of detail provides two benefits. The data enable your organization to identify which vulnerabilities affect particular subsets of the IT infrastructure. An accurate inventory ensures that you select and apply the correct patches during remediation. The tracking inventory also helps speed the scanning process because it limits scans to relevant devices, software and services affected by particular vulnerabilities. Discovering devices, software and services and tracking this inventory can be done manually. You can also automate the entire discovery and tracking inventory process with an on demand vulnerability management service like QualysGuard.

Scan systems for vulnerabilities

A vulnerability scan tests the effectiveness of security policy and controls by examining network infrastructure for vulnerabilities. The scan systematically tests and analyzes IP devices, services and applications against known security holes. A post-scan report reveals actual vulnerabilities and states what needs fixing. There are many options for scanning. Some require software applications you install and maintain, such as the Nessus public domain scanner. These require lots of time and carry typical operational overhead. A Web-based on demand solution such as QualysGuard does the scans for you over the Internet. It works without special software or hardware. Another advantage to a Web-

based service is being always up-to-date with the most recent vulnerabilities. You shouldn't have to worry about updates to scanning technology because it's a key part of the vulnerability management system.

Compare vulnerabilities against inventory control list

The comparison process helps to minimize false positives. With some vulnerability scanning and intrusion detection systems, for example, false positives can dwarf accurate alarms if vulnerabilities do not match what's in your inventory. To eliminate inaccurate hits and the resulting waste of time chasing down false positives, compare your organization's IP inventory against industry standard vulnerability databases such as the Common Vulnerabilities and Exposures (www.cve.mitre.org) list and NIST's ICAT Metabase (www.icast.nist.gov). CVE provides a comprehensive list of publicly known vulnerabilities, an analysis of authenticity of new vulnerabilities, and a unique name for each vulnerability. ICAT takes CVE to the next level with detailed information about each vulnerability. Also use the SANS Top 20 and CERT Advisories (www.scans.org/top20.html and www.cert.org/advistories/). QualysGuard automatically does the comparison against industry standard vulnerability databases and other public and private lists of vulnerabilities.

"As a Web-based solution, QualysGuard enables us to perform security audits as often as necessary, spot vulnerabilities immediately as they are added to the QualysGuard database, and work proactively to remediate them. This helps us secure all our network entry points, enforce ICI security policies and assists us in meeting federal requirements."

Paul Simmonds
Dir. of Global Information Security
ICI

Classify the risk

It is practically impossible to fix everything at once. So this vulnerability management process ranks vulnerabilities to determine what to fix first. Organizations can devise their own category scheme or adopt rating scales from other sources. Microsoft Corp., for example, publishes four categories of risk: Critical, Important, Moderate and Low with corresponding rates of remediation (www.microsoft.com/technet/community/columns/secmgmt/sm0404.mspx?pf=true). QualysGuard automatically assigns a category and a severity level for each vulnerability detected. Its category ratings are Vulnerability, Possible Threat, or Information Gathered or Service. A severity level indicates the security risk posed by exploitation of the vulnerability and its degree of difficulty. The results of successful exploitation of vulnerability can vary from disclosure of information about the host to a complete compromise of the host (www.qualys.com/research/rnd/knowledge/severity/).

Pre-test the patch or other remediation

Patching vulnerabilities is not like bandaging a wound or spackling a small hole. It's more like surgery. After software vendors rewrite pieces of an application, the resulting "healed" software compilation is still vulnerable to other bugs. Software always has and always will have bugs, so organizations should pre-test patches before applying them to live systems. Some faulty patches have crashed business processes (see "Users pressure Microsoft on tests in wake of Sasser," 11 May 2004, *ComputerWeekly.com*). Testing should occur in your organization's environment. Most problems with patches are due to third-party applications or modifications to default configuration settings. Organizations should verify cryptographic checksums, Pretty Good Privacy signatures and digital certificate to confirm authenticity. Verify that the patch corrects the vulnerability without affecting operations of the business process and applications.

Apply the patch

Fixing security problems is the result of vulnerability management. Traditional manual processes for applying patches and other remediation are slow and expensive. Sometimes the high cost of patching coupled with the high volume of patches released by vendors encourages organizations to delay remediation. Organizations may delay updates – even for critical patches – until multiple patches or service packs are available, or until arrival of a regular monthly, quarterly or annual update process. Unfortunately, delay can be a fatal strategy

so it's important to remediate vulnerabilities as quickly as possible. Automated patch management and software distribution solutions can help speed this process and keep costs to a minimum. Rollback capability allows organizations to efficiently ensure use of appropriate software versions. Integrating patch management with other automated vulnerability management processes is beneficial. Open XML application programming interfaces enable integration of QualysGuard with third party remediation and patch management software such as Arcsight, Citadel and GuardedNet.

Re-scan for vulnerability and confirm the fix

After application of a patch or remediation process, organizations should rescan IP-connected assets to ensure that the fix worked and that it does not cause other network devices, services or applications to malfunction. Verification of fixes with resulting scan reports provides documentation for compliance with security provisions of laws and regulations such as Gramm-Leach Bliley, HIPAA and Sarbanes-Oxley.

"Proactive vulnerability assessment is a necessity to protect our business form zero-day exploits, worms, and hackers. We use QualysGuard to audit business-critical assets in order to protect our brand and our shareholders against potential financial loss."

Dan Klinger
Chief Information Security Officer
Hershey Foods

GUIDELINES FOR EFFECTIVE REMEDIATION

Vulnerability management will help your organization to identify all known risks, minimize false positives and effectively remediate vulnerabilities. The following guidelines will help implement better processes for vulnerability management.

Standardize and Approve Processes

Focus on articulating processes before implementing tools. Your organization's strategy needs approval by senior management. In some cases, application of a patch may require temporarily pausing a business process. Security administrators must have approval to stop business cash flow for emergency patching. Executives should approve in advance how vulnerability remediation works in an emergency.

Make Processes Efficient

Look to automate as much as possible for efficiency. QualysGuard eases vulnerability management by automating most of the processes. For remediation, batch software updates whenever you can to avoid multiple reboots and minimize downtime. Gradually, new installers will use hot patching update code in memory. This technique doesn't replace code on the disk until you shut down the service or application. Another new technique called warm patching will shut down the service before patching to avoid rebooting after you apply the patch.

Preserve Uptime

Sometimes remediation requires taking a system offline to apply a patch. Patching processes should preserve uptime. Organizations using a N+1 Web architecture can use load balancing to preserve uptime by taking boxes off line for patching one at a time during non-peak hours.

Simplify Environments

Vulnerability management is easier and faster when systems use similar configuration. Complexity of IT environments slows the cycle of creating security policies and controls, tracking inventory, scanning systems for vulnerabilities, comparing vulnerabilities against inventory, classifying risks, pre-testing patches and other remediation, and re-scanning.

QUALYSGUARD ON DEMAND VULNERABILITY MANAGEMENT

14-Day Free Trial

Identify all known risks

Minimize false positives

Fix vulnerabilities fast

Consistently doing vulnerability management will help your organization to prevent damage from viruses, worms and other network-borne attacks and keep business systems operating without interruption. Automation helps make the processes of vulnerability management more accurate, timely and cost-efficient. Automation with solutions like QualysGuard helps ensure completion of all the processes for the best protections. Vulnerability management with QualysGuard also provides documented compliance with laws and regulations for security, personal privacy and corporate governance.

Experience the benefits of on demand vulnerability management with a free, 14-Day Trial of QualysGuard. Here are the easy steps:

1. Complete a short form at http://www.qualys.com/forms/?lsid=6466 or call a Qualys sales representative at **800.745.4355**.
2. Qualys will assign an account name and password for the free trial.
3. Use your login and password to launch your trial.
4. View the scan's audit results online, read suggested solutions, download patches and fix security problems.
5. Repeat scans as often as you like for fourteen days.

ABOUT QUALYS, INC.

Qualys is the leader in on demand vulnerability management. The company allows organizations of all sizes to effectively secure their network, conduct automated security audits, and ensure compliance. Qualys automates the process of proactively identifying and remediating security vulnerabilities, and provides the quickest route to neutralize worms and other emerging threats according to their relative business impact. Qualys' on demand technology offers customers significant economic advantages, requiring no capital outlay or infrastructure to deploy and manage. Its distributed scanning capabilities and unprecedented ability to scale make it ideal for large, distributed organizations. Thousands of customers rely on Qualys, including DuPont, Hershey Foods, Hewlett-Packard, Standard Chartered Bank and many others. Qualys is headquartered in Redwood Shores, Calif., with European offices in France, Germany and the U.K. and Asian offices in Japan, Singapore, Australia, Korea and the Republic of China.

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