

THE NEED FOR VULNERABILITY MANAGEMENT

Table of Contents

Intro	2
The Prevalence of Network Vulnerabilities	2
Recent Changes in Vulnerability Attacks	3
VM Controls the Removal of Vulnerabilities	4
VM Documents Compliance	6
QualysGuard Automates Key VM Technology and Workflow	8
About Qualys	9



Vulnerability Management Primer

WHAT

VM is the process of finding and fixing mistakes in software and configuration errors.

WHY

New vulnerabilities appear every day; automation is required to speed remediation.

HOW

A combination of software tools and VM workflow.

BENEFITS

Proactive protection from attacks; documented assurance that the network is safe and compliant.

To a cyber criminal, vulnerabilities on a network are hidden, high-value assets. Their targeted exploitation may result in unauthorized entry into a network, which can expose confidential information, provide fuel for stolen identities, cause theft of business secrets, violate privacy provisions of laws and regulations, or paralyze business operations. New vulnerabilities appear every day due to flaws in software, faulty configuration of applications and infrastructure, and human error. Whatever their source, vulnerabilities do not go away by themselves. Their detection, removal and control require vulnerability management (VM) – the calibrated, continuous use of software tools and workflow that proactively purges exploitable risks.

This guide describes the need for VM. It introduces the sources of vulnerabilities and their related fallout, then relates why the nature of modern threats to the network requires automated technology to counter sophisticated exploits. The guide defines elements of VM and how it controls the detection and remediation process. As an important byproduct, VM can also document compliance with security provisions mandated by legislation, industry and business policy. VM can be implemented for networks of all sizes with cost-effective technology that automates much of what used to be a complex, manual process. The assurance of security provided by VM prevents fallout from malicious exploits and preserves continuity of business operations.

The Prevalence of Network Vulnerabilities

Vulnerabilities have plagued operating systems and software applications from the earliest days of computing, but the main accelerant to exploitation by hackers and criminals is universal connectivity over the Internet. This global pathway provides access to networks and their computing resources. When network-attached devices have unpatched vulnerabilities, they are susceptible to a variety of exploits.

Programming mistakes cause most vulnerabilities in software. A common mistake is failure to check the size of data buffers; their overflow can corrupt the stack or heap areas of memory, which may allow the execution of an attacker's code on that machine via a virus, worm or other exploit vector. The standard assumption by computer scientists is 5 to 20 bugs in every thousand lines of software code, so it is no surprise to see regular announcements of new vulnerabilities with related patches and workarounds. The risk of unanticipated vulnerabilities grows with use of General Public License software, particularly as implementers plug in untested modules of object-oriented programming code. These modules may include non-robust implementations of Internet protocol standards, making them susceptible to attack when placed into production environments.

Careless programmers are not the only source of vulnerabilities. For example, improper configuration of security applications such as a firewall may allow attackers to slip through ports that should be closed. Users of mobile devices may use a website without going through the corporate VPN, thus exposing those devices and the network to attacks. Or, a vector of attack may occur by clicking on an email attachment infected with malware. The exploitation of vulnerabilities via the Internet is a huge problem requiring immediate proactive control and management.

Recent Changes in Vulnerability Attacks

Ease of Deployment

Endless public disclosures of data breaches have revealed exposure of millions of confidential consumer records – adequate proof why organizations must do more to protect networks from attack. But a dramatic change in the security threat landscape is raising the bar for organizations who want to actively minimize successful exploits of vulnerabilities.

Recent data show that exploits are no longer restricted to traditional risks of generic viruses, worms, Trojans and other single-vector attacks. According to global research by Symantec Corporation, a fundamental change in threats reveals movement “away from nuisance and destructive attacks towards activity motivated by financial gain.”¹ Its report characterizes five new trends:²

- **Increased professionalism and commercialization of malicious activities**
- **Threats that are increasingly tailored for specific regions**
- **Increasing numbers of multistaged attacks**
- **Attackers targeting victims by first exploiting trusted entities**
- **Convergence of attack methods**

Respondents to the *2007 CSI Computer Crime and Security Survey* report that financial fraud causes the highest dollar amount of losses (31% of total), compared to viruses/worms/spyware (12%), system penetration by an outsider (10%), or theft of confidential data (8%).³

The fallout from cyber attacks now poses serious financial risk, so many organizations have taken steps to mitigate malware and other vectors of attack by deploying layers of security technology such as anti-virus/anti-spyware software, firewall, intrusion detection/prevention, VPN and encryption. Technologies like these are essential components of network security, yet while they are effective in their own spheres of purpose, none perform the most fundamental of all security measures: vulnerability management.

1 Symantec Internet Security Threat Report, Trends for January – June 07, Executive Summary, p. 2.

2 Ibid.

3 2007 CSI Computer Crime and Security Survey, p. 15.

Malicious Activity by Country

Overall Rank	Previous Rank	Country	Overall Proportion	Previous Overall Proportion	Malicious Code Rank	Spam Zombies Rank	Command-and-Control Server Rank	Phishing Web sites	Bot Rank	Attack Rank
1	1	United States	30%	31%	1	1	1	1	2	1
2	2	China	10%	10%	2	3	5	18	1	2
3	3	Germany	7%	7%	7	2	2	2	3	3
4	5	United Kingdom	4%	4%	3	15	6	3	7	5
5	4	France	4%	4%	9	7	12	6	5	4
6	7	Canada	4%	3%	6	31	3	7	8	7
7	8	Spain	3%	3%	10	10	22	13	4	6
8	10	Italy	3%	3%	5	6	8	12	6	8
9	6	South Korea	3%	4%	26	8	4	10	13	12
10	11	Japan	2%	2%	4	20	13	8	16	10

Source: Symantec Corporation

VM Controls the Removal of Vulnerabilities

Vulnerability management has evolved from simply running a scanner on an application, computer or network. Scanning is an essential element of vulnerability management, but VM includes other technologies and workflow that contribute to a bigger picture required for controlling and removing vulnerabilities. The primary objectives of VM are:

- **Fix faults in the software affecting security, performance or functionality.**
- **Alter functionality** or address a new security threat, such as updating an antivirus signature.
- **Change a software configuration** to make it less susceptible to attack, run faster or improve functionality.
- **Use most effective means** to thwart automated attacks (worms, bots, etc.)
- **Document** the state of security for audit and compliance with laws, regulations and business policy.

Consistent, ongoing execution of vulnerability management is difficult, if not impossible to do on a manual basis. There are simply too many “moving parts” to juggle and act on in a timely and cost-effective manner. For this reason, organizations should look to automate as much as they can for each element of VM. The rest of this section describes how the function of VM technologies and workflow help to control and remove network vulnerabilities.

QualysGuard Automates VM Workflow

1. Track inventory and categorize assets
2. Scan systems for vulnerabilities
3. Compare vulnerabilities against inventory
4. Classify and rank risks
5. Pre-test patches, fixes and workarounds
6. Apply patches, fixes and workarounds
7. Re-scan to confirm fixes and verify security

Track Inventory and 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 and fixes during remediation. The tracking inventory also helps speed the scanning process because it limits scans to devices affected by particular vulnerabilities.

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. Another option is using a third party scanning service over the Internet, which automates all operations and lowers related costs.

Compare Vulnerabilities Against Inventory

The next step in vulnerability management workflow is a comparison process to minimize false positives. Some vulnerability scanning and intrusion detection systems generate many false positives, which drown the accuracy of alarms if they do not match what's in your inventory. To eliminate the time-wasting process of 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 the NIST National Vulnerability Database (<http://nvd.nist.gov>). The NIST database takes CVE to the next level with detailed information for each of its vulnerabilities. Other databases include the SANS Top 20 and CERT Vulnerability Notes (www.sans.org/top20 and www.kb.cert.org/vuls/).

Classify and Rank Risks

It is practically impossible to fix everything at once. This workflow process ranks vulnerabilities to determine what to fix first. Organizations can devise their own category scheme or adopt rating scales from other sources.

Pre-Test Patches, Fixes and Workarounds

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.

Making VM Easier

VM Solutions Integrated with QualysGuard API

- Security Information & Event Management
- Patch Management
- Help Desk
- Risk Management
- Network Access Control
- IDS/IPS
- Network Patching
- Security Policy Management
- Penetration Testing

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. 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 certificates to confirm authenticity. Verify that the patch corrects the vulnerability without affecting applications and operations of the business process.

Apply Patches, Fixes and Workarounds

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 availability of multiple patches, service packs, or 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.

Re-scan to Confirm Fixes and Verify Security

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.

VM Documents Compliance

A major benefit of vulnerability management is the automatic provision of documentation to validate compliance. Organizations are required by law to comply with a growing number of government and industry-specific regulations for safeguarding the confidentiality, integrity and availability of electronic data from information security breaches. Organizations that do not fully comply and stay up-to-date with security regulations face serious potential consequences – including fines, civil, and sometimes criminal penalties.

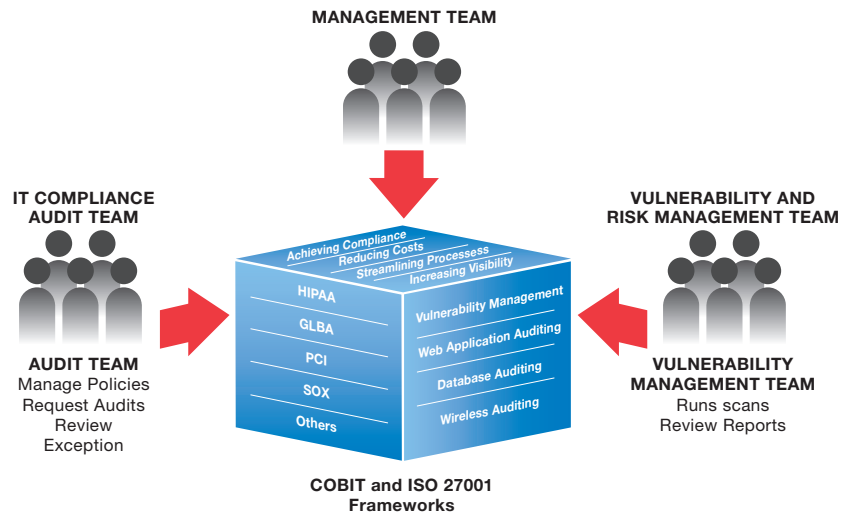
Documentation usually consists of reports from scanning and patch management systems. These reports document network security audits and remediation, including detailed, prioritized lists of existing vulnerabilities related to severity of risk, and verification of vulnerabilities that were fixed with patches or workarounds.

“Vulnerability management reports from QualysGuard help give outside auditors the knowledge that we’re being proactive and taking security problems seriously.”

Senior Manager, Information Security
eBay Inc.

VM Documentation Verifies Compliance with Organization Policy

At the most basic level, VM documentation must verify compliance with security policies defined by an organization. Automated VM processes facilitate policy oversight and management. VM reports are used to document and demonstrate security policy compliance to internal and external auditors.



VM Documentation Verifies Compliance with Regulations

Healthcare – HIPAA regulates the security and privacy of health data, including patient records and all individually identifiable health information.

Financial Institutions – Regulations such as the Basel II, MiFID, LSF and GLBA require IT controls to reduce risk and maintain the confidentiality and privacy of financial information.

Merchants – The Payment Card Industry, including American Express, Discover, JCB, MasterCard and Visa International mandate the protection of cardholder data residing with merchants, safe from hackers, viruses and other potential security risks.

Public Companies – Sarbanes-Oxley requires effective controls and processes for validating the integrity of annual financial reports.

Government – FISMA requires that federal agencies establish risk-based information security programs to secure federal information.

Other – The Data Protection Act of 1998 is a UK Act of Parliament and creates rights for those who have their personal data collected and stored. CNIL (France) provides similar protection. While, CA 1798.82 mandates that organizations doing business in California report any cyber security breaches that may have comprised customer information.

“QualysGuard has allowed us to be very focused on the risks that matter.... [and] has really helped raise our level of compliance across our entire environment.”

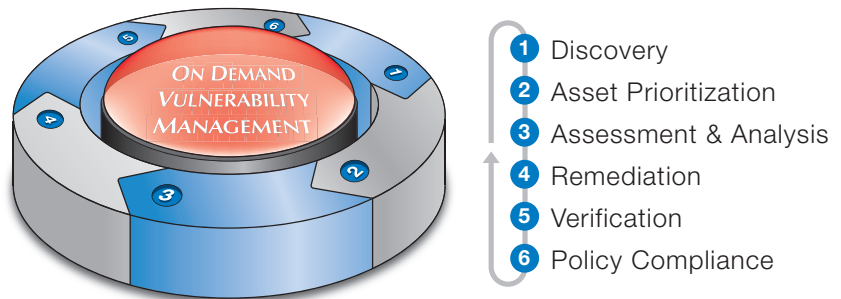
Chief Information Protection Officer
CIGNA Corporation

QualysGuard Automates Key VM Technology and Workflow

QualysGuard enables organizations to reduce risk and manage compliance processes by providing vulnerability management and policy compliance in one solution. QualysGuard automates the process of VM and policy compliance across the enterprise, providing network discovery and mapping, asset prioritization, vulnerability management assessment reporting and remediation tracking according to business risk. Policy compliance features allow security managers to audit, enforce and document compliance with internal security policies and external regulations.

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

QUALYSGUARD VULNERABILITY MANAGEMENT LIFECYCLE



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

About Qualys

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

To learn more about QualysGuard, visit: www.qualys.com.



USA – Qualys, Inc. • 1600 Bridge Parkway, Redwood Shores, CA 94065 • T: 1 (650) 801 6100 • sales@qualys.com
UK – Qualys, Ltd. • 224 Berwick Avenue, Slough, Berkshire, SL1 4QT • T: +44 (0) 1753 872101
Germany – Qualys GmbH • München Airport, Terminalstrasse Mitte 18, 85356 München • T: +49 (0) 89 97007 146
France – Qualys Technologies • Maison de la Défense, 7 Place de la Défense, 92400 Courbevoie • T: +33 (0) 1 41 97 35 70
Japan – Qualys Japan K.K. • Pacific Century Place 8F, 1-11-1 Marunouchi, Chiyoda-ku, 100-6208 Tokyo • T: +81 3 6860 8296
Hong Kong – Qualys • 2/F, Shui On Centre, 6-8 Harbour Road, Wanchai, Hong Kong • T: +852 3163 2888

