Guide to Effective Remediation of Network Vulnerabilities and Compliance

Table of Contents

QUALYSGUARD AUTOMATES THE VULNERABILITY MANAGEMENT PROCESS

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

I. Overview

Remediation of network vulnerabilities before exploits strike is the golden ideal for every organization. Proactive remediation strengthens security by removing the exploitability of assets. This is the safest of all states, and helps to ease a traditional reliance as the primary protection against hackers and other network-borne threats. Documentation of regular, ongoing vulnerability remediation is also a common network security requirement of laws and regulations such as PCI, GLBA and HIPAA.

While remediation is the ideal, cyber thefts of tens of millions of personal and corporate records at TJX Companies, DSW Inc., CardSystems Solutions, Inc. and many others show that some organizations need to work harder at proactive security. Effective remediation entails continuous processes that together are called Vulnerability Management. The workflow and related technology defined by vulnerability management help organizations to efficiently find and fix network security vulnerabilities and document compliance. This guide describes the major workflow processes of vulnerability management and how QualysGuard, as an on demand software-as-a-service (SaaS) automates most of these for fast, cost-effective remediation and compliance documentation.

II. Vulnerability Management Improves Security

Most remediation entails fixing mistakes in software. The standard assumption of 5 to 20 bugs in every thousand lines of software code means risk is soaring as implementers of large new object-oriented applications tap untested modules and protocols. Realistically, software bugs will always be a problem so proactively detecting and fixing issues will continue to be an organizational priority. Vulnerability management is done to:

- ***Fix faults in the software affecting security, performance or functionality.***
- ***Alter functionality*** or to address a new security threat, such as by 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 (e.g. worms, bots, DOS, etc.).
- ***Document*** the state of security for audit and compliance with laws, regulations and business policy.

III. Automating Vulnerability Workflow Is Crucial

Consistent, ongoing execution of vulnerability management and policy compliance 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. QualysGuard allows organizations to automate most workflow elements for vulnerability management and policy compliance – particularly the most time consuming and manually error-prone.

QualysGuard Automates Steps of Vulnerability Management

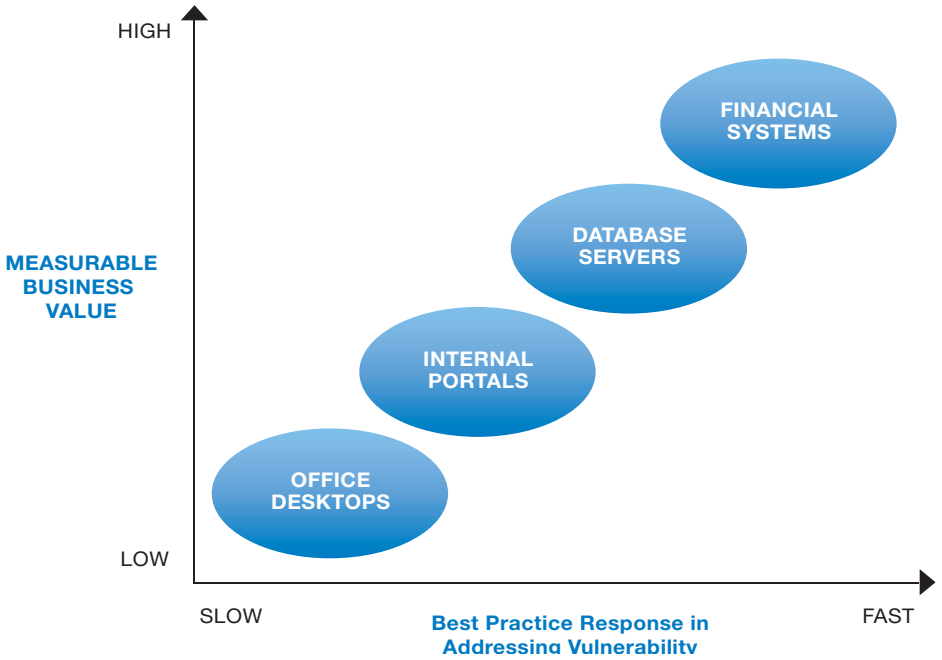
> *"Enterprises that implement a vulnerability management process will experience 90% fewer successful attacks than those that make an equal investment only in intrusion detection systems."*
>
> **Gartner, Inc.**

#1 Create Security Policies and Controls

Policy creation and management is a critical first step for organizations. 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 detection/prevention. Policies and controls should include servers, network services, applications and endpoints. Policy management used to be a manual, cumbersome process. New software tools can automate policy management and enforce configurations on endpoint devices. Automation saves time, improves accuracy and lowers total cost of ownership. QualysGuard helps execute security policies by testing controls, quickly identifying and remediating vulnerabilities, and documenting compliance. The QualysGuard API enables data from QualysGuard to automatically funnel into third-party solutions for policy management, risk correlation and enterprise security management.

#2 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 in order to prioritize their vulnerability remediation efforts. Elements in the database include all hardware, software, applications, services and configurations. Tracking this level of detail provides two benefits. The data enables your organization to identify which vulnerabilities affect



> *"The automated scans provide much more efficiency than the manual scans we conducted in the past. And our weekly QualysGuard reports provide us the insight into risk that we need to know."*
>
> Network Security Engineer
> **SAS Institute**

particular subsets of the IT infrastructure. In addition, an accurate inventory ensures that the correct patches are selected and applied during remediation. The tracking inventory also helps speed the scanning process because it limits scans to devices affected by particular vulnerabilities. You can track this data manually, but vulnerability management is much more effective by automating the entire discovery and tracking inventory process on demand using QualysGuard.

#3 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 for 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 significant time, resources and carry typical operational overhead. By contrast, QualysGuard performs the scans for you on demand over the Internet. As a SaaS-based solution, the QualysGuard service works without special software and is always up-to-date with the most recent vulnerability signatures. As a result, you don't have to worry about updates to scanning technology because it's a key part of QualysGuard's vulnerability management system.

#4 Verify Vulnerabilities Against Inventory

An important workflow sub-process of scanning requires verifying that vulnerabilities match the actual devices, software and configurations in your network. The value of this step is to minimize efforts spent investigating risks that do not apply to your network configuration. False positives inhibit some vulnerability scanning and intrusion detection systems by drowning the accuracy of alarms with alerts that do not match what's in your inventory. To eliminate the time-wasting process of chasing down false positives, Qualys' vulnerability management process scans your organization's IP inventory against the most comprehensive vulnerability database in the industry – producing scan results with a Six-Sigma accuracy rate. QualysGuard vulnerability intelligence includes sources 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 Qualys sources include the SANS Top 20 and CERT Vulnerability Notes (www.sans.org/top20 and www.kb.cert.org/vuls/). Collectively, all this is brought into the Qualys Knowledgebase as QualysGuard automatically compares network inventory against all of these industry standard vulnerability databases and as well as private lists of vulnerabilities. The result is accurate, concise information that you can trust and applies to assets in your organization.

Other Solutions Integrated with QualysGuard

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

#5 Classify and Rank Risks

It is practically impossible to fix everything at once. In fact, in large organizations, the amount of vulnerability data can be overwhelming if it is not properly categorized, segmented, and prioritized in a meaningful fashion. The QualysGuard workflow 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 (www.microsoft.com/technet/community/columns/secmgmt/sm0404.mspx?pf=true) remediation. 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 can vary from disclosure of information about the host to a complete compromise of the host (www.qualys.com/research/rnd/knowledge/severity/). QualysGuard automates the entire process and provides relevant, actionable information that you can trust.

#6 Pre-Test Patches, Fixes and Workarounds

After software vendors rewrite pieces of an application, the resulting “healed” software compilation (or patch) can still vulnerable to other bugs. As a result, 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 unique 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. Pre-classified and ranked vulnerability data from QualysGuard is automatically integrated by several third-party patch automation solutions.

#7 Apply Patches, Fixes and Workarounds

Finding and fixing security problems is the core of vulnerability management. Traditional manual processes for finding flaw, suggesting patches and other remediation actions are slow, error-prone and expensive. Sometimes the high cost of patching coupled with the high volume of flaws detected in vendor applications 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 as potential threats are quickly detected by attackers as the window between flaw and exploit is

> *"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.**

constantly shrinking. Therefore, it's important to remediate vulnerabilities as quickly as possible and minimize risk. 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. QualysGuard provides one-click links to vulnerability patches, fixes and workarounds to be used during this phase of workflow.

#8 Re-Scan to Confirm Fixes and Verify Compliance

> *"Using Qualys was easy to sell [internally] because every business unit could immediately put the vulnerability management service to work without requiring more internal resources."*
>
> Director, Technology Services
> **RR Donnelley**

After application of a patch or completion of the 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 PCI-DSS, HIPAA, Gramm-Leach-Bliley, and Sarbanes-Oxley. Similar reports should also confirm compliance with internal operating policies. QualysGuard automates the creation of reports for many laws and regulations, and provides simple customization features for documenting compliance with any business policy.

VI. QualysGuard – SaaS-based Vulnerability Management for Stronger Security & Verification of Compliance

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 allows organizations to:

- ***Discover and manage all devices and applications on the network***
- ***Identify and remediate network security vulnerabilities***
- ***Measure and manage overall security exposure***
- ***Ensure compliance with internal policies and external regulations***

> *"Before QualysGuard we had an ad hoc process; Qualys brought much stronger control & visibility into our processes."*
>
> Information Protection Director
> **CIGNA Corporation**

V. 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.

QUALYS®
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

ON DEMAND SECURITY