CONTINUOUS MONITORING

A New Approach to Proactively Protecting Your Global Perimeter

QUALYS®

CONTINUOUS SECURITY

TABLE OF CONTENTS

In a perfect world, your network would have an always-on, continuous view of your global network perimeter. This requirement is for threat actors who can launch sophisticated attacks from any global location at any time. Your network security controls must have the ability to automatically identify and repel any attack, prevent operational interruptions, and protect the confidentiality, integrity and availability of critical applications and data. Achieving this state is the Holy Grail of security and continuous monitoring is a vital step toward accomplishing this goal.

This guide describes the need for continuous monitoring and offers a blueprint for creating a continuous security practice. As a result, continuous monitoring will give your organization the most comprehensive view of its global perimeter, and empower you to proactively identify and address potential threats enabled by vulnerabilities in software or weak system configurations.

THE NEED FOR CONTINUOUS MONITORING

Agile business processes such as cloud computing and virtualization have transformed the old static nature of an enterprise network perimeter. Now the perimeter is distributed, complex and highly dynamic with independent operational teams managing and changing configurations to firewalls, routers, switches, load balancers, hosts, applications, and other systems. Perimeter scanning and response to unintentional security holes created by these changes is often event-driven and only performed at designated times – typically intervals of every week or month. This presents a significant opportunity for cybercriminals to exploit newly introduced vulnerabilities and infiltrate networks in between scans. Also, new vulnerabilities in software for devices and applications are discovered every day, which is another source of threats that can exploit operational configurations changing by the minute.

For example, a University of Michigan study, "How Vulnerable are Unprotected Machines on the Internet?" found servers with open ports and other vulnerabilities were scanned within about 23 minutes of being attached to the Internet and vulnerability probes started in 56 minutes. Average time to the first exploit was less than 19 hours. To quickly and proactively prevent exploits, organizations need a new operational defense strategy: Continuous Monitoring. Continuous Monitoring means what it says – the process of vigilance must never stop, so that strategic high priority assets get immediate attention from first responders on operations teams in order to prevent security exploits. Frequent scanning with the award winning Qualys Vulnerability Management web service is a vital foundation. But there is a new, automated approach that can take your organization's vigilance to the next level: Qualys Continuous Monitoring (CM).

HOW OFTEN SHOULD YOU SCAN?

At a minimum, Qualys urges you to scan your entire network at least daily.

Asset inventory, configuration and vulnerability data gathered by Qualys Vulnerability Management is the raw fuel of Qualys Continuous Monitoring. Without fresh data, monitoring is not "continuous" and your network is at risk.

Strategic, high-value assets should be scanned multiple times a day – or better yet, continuously by using the "Continuous Scanning" feature of Qualys Vulnerability Management.

Read How To Configure Continuous Scanning here:
https://community.qualys.com/docs/DOC-3852

CM AND VULNERABILITY MANAGEMENT

Qualys Continuous Monitoring provides organizations with a comprehensive, always-on view of potential security holes, empowering them to immediately identify and proactively address potential vulnerabilities before they turn into breaches. Built on the Qualys Cloud Platform, Qualys Continuous Monitoring uses its elastic scanning capacity to dynamically scale to networks of any size and scope. The key benefit is instantly alerting first responders on operational teams as soon as an unauthorized change is detected.

There is a deep, symbiotic relationship between Qualys Continuous Monitoring and Qualys Vulnerability Management. Vulnerabilities may consist of software-borne threats such as worms, viruses and others; they also may stem from issues related to configurations of your IT environment. The merger of both scenarios is a toxic combination of threats requiring continuous monitoring and remediation. The whole idea of continuous monitoring hinges on the availability of timely, accurate data about your IT environment – including changes to systems and configurations that expose new vulnerabilities. These data are automatically collected and analyzed during scans. Continuous monitoring is the next step of immediately putting this information into the hands of first responders for judgment and action.

Transforming the old model. Qualys CM transforms the old scanning-and-report driven process by parsing scan results by your criteria, and automatically alerting appropriate first responders with specific information tailored for the respective assets assigned to their responsibility. The old way entailed passing a big, often arcane report through a bureaucracy of managers, supervisors and technicians. As a result, the velocity of remediation was often way behind threats appearing by the minute.

Qualys CM sends “Twitter-like” bursts of essential information quickly into the hands of the right people for immediate and targeted action. This service accelerates the ability of first responders to stay ahead of threats to the most important assets. Qualys CM lets you granularly control the intervals and targets of notification; we describe this in more detail later in the guide.

Frequent scans make continuous monitoring effective. The frequency of vulnerability scanning is what fuels the effectiveness of alerts by Qualys CM. For example, if you scan once a quarter or even once a month, having the ability to “continuously monitor” data from those scans is hardly up-to-date when vulnerabilities change by the minute on a giant, fluid attack surface. Given the continuous change in threats, Qualys suggests scanning your network at least daily, and more often for critical, high-priority assets (see sidebar on page 3). As a result, vulnerability scanning data will truly be up-to-date, which enables Qualys CM to be a useful – and vital – component of keeping your network safe from exploits.

CRITICAL SECURITY CONTROLS AND GUIDANCE FOR CM

Qualys is not the only one recommending frequent scanning and continuous monitoring. For several years, the National Institute of Standards and Technology (NIST) has advised federal agencies to use continuous monitoring as an important process for managing risk. NIST Special Publication 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations,* specifies related procedures for compliance with FISMA, the *Federal Information Security Management Act*. Establishing monitoring and assessment frequencies are stated as "critical functions" (p. 25), and higher frequencies are urged for critical systems (pp. 25-27). Implementing this guidance has been difficult until the availability of Qualys CM.

Other guidance is from the Critical Security Controls (formerly known as the "SANS 20 Critical Controls"), which are a prioritized, risk-based approach to cyber security. They are the result of a consensus process that involved a wide variety of cyber security professionals from government and industry who were asked: "In practice, what works and where do you start?" The Critical Security Controls (CSCs), now managed by the Council on Cybersecurity, of which Qualys is a founding member and active participant in developing CSCs, have become a blueprint to help Chief Information Security Officers (CISOs) and Chief Information Officers (CIOs) to deploy the most effective processes and tools to secure all their computer systems according to risk.

For example, the CSCs advise that any unauthorized machine connected to the Internet be identified within 24 hours, and patching vulnerabilities in critical operating systems and applications should occur within 48 hours.

THE CRITICAL SECURITY CONTROLS RECOMMEND:

Scanning – automatic vulnerability scans should be weekly or more frequent.
Alerts – effectiveness should be measured in minutes.
Discovery – unauthorized hosts should be identified within 24 hours.
Patching – should occur within 48 hours for critical systems.

Source: Critical Security Controls managed by the Council on Cybersecurity

CSC 4 is Continuous Vulnerability Assessment and Remediation. It recommends automatic vulnerability scans be done on a weekly or more frequent basis. It urges organizations to measure the effectiveness of resulting alerts "in minutes" as time is of the essence for continuous monitoring.

How Qualys Continuous Monitoring fulfills this requirement

- Qualys Vulnerability Management scans periodically (by schedule) for vulnerabilities on all network-connected systems.
- Qualys also provides scans on demand for ad hoc checks, or for specific vulnerabilities such as "forbidden ports," which is recommended by CSC 4.
- The solution also supports continuous scanning for mission-critical systems and sub-networks.
- Qualys reports vulnerabilities in patch-centric views using "supersede" information to help boost efficiency in scanning and remediation.
- Reports integrate CVE and CVSS standards for flexible analysis of results.
- Remediation tracking with an internal ticket system provides visibility and control for ensuring the safety of vital systems and networks.
- Qualys CM provides immediate notification of vulnerabilities and remediation paths to first responders.

For more information on CSCs, see http://www.CouncilOnCybersecurity.org/critical-controls.

HOW TO EFFECTIVELY USE QUALYS CM

Qualys Continuous Monitoring is a SaaS-based add-on purchase used with Qualys Vulnerability Management. Qualys CM provides powerful configuration options that scale to custom requirements of large enterprises. Three themes guide the configuration strategy for effective use of Qualys CM: Where, What, and Who.

Where Qualys CM is applied. Your organization needs to prioritize assets for priority attention when Qualys CM notifies your team of an incident requiring remediation. You already should be using asset prioritization with Qualys Vulnerability Management, which enables assignment of custom weighted values denoting the business value of critical assets. This information can be leveraged in Qualys CM and is managed with Monitoring Profiles. A profile can be applied to a single host, or to a group of hosts using Asset Tags or by manually entering IP ranges. The profiles ensure that first responders address high priority assets.

What Qualys CM looks for on your network. Your team of first responders leverages the ability of Qualys CM to pinpoint issues that are of special interest for network security. These are controlled by Rule Sets, which are easily configured for common classes of vulnerabilities – including unique requirements. A Rule Set can be created from scratch or re-use existing criteria selected by Asset Tags. Typically these may include:

- **Host** – Qualys CM detects whenever systems appear, disappear, or are running unexpected operating systems. The recipient of an alert can quickly drill down to inspect all related data gathered by Qualys Vulnerability Management. These include a summary of name, IP address, DNS name, NetBIOS name, and operating system; open ports; installed software; vulnerabilities affecting the host; and a history of alert notifications that provide context on whether the host has been persistently ridden with vulnerabilities.
- **OS Changes on Existing Hosts** – Qualys CM notifies when changes have been made to operating systems on existing hosts.
- **Vulnerability** – When vulnerability remains open, Qualys CM notes it as “active” and requires remediation. New, re-opened and closed vulnerabilities are also noted.
- **SSL Certificate** – Qualys CM identifies certificates that have expired, are soon-to-expire, rogue or unknown – all of which are potential triggers to stop ongoing operations of your network’s services and applications.

- **Port or Service** – Newly opened ports, changes to ports, new services on ports, and closing of ports common vectors for attack and exploit. Qualys CM notes all these events and alerts you accordingly.
- **Software** – Installation of new or unauthorized software, upgrades or downgrades of existing software, and removals can also weaken the perimeter attack surface and is addressed by Qualys CM.

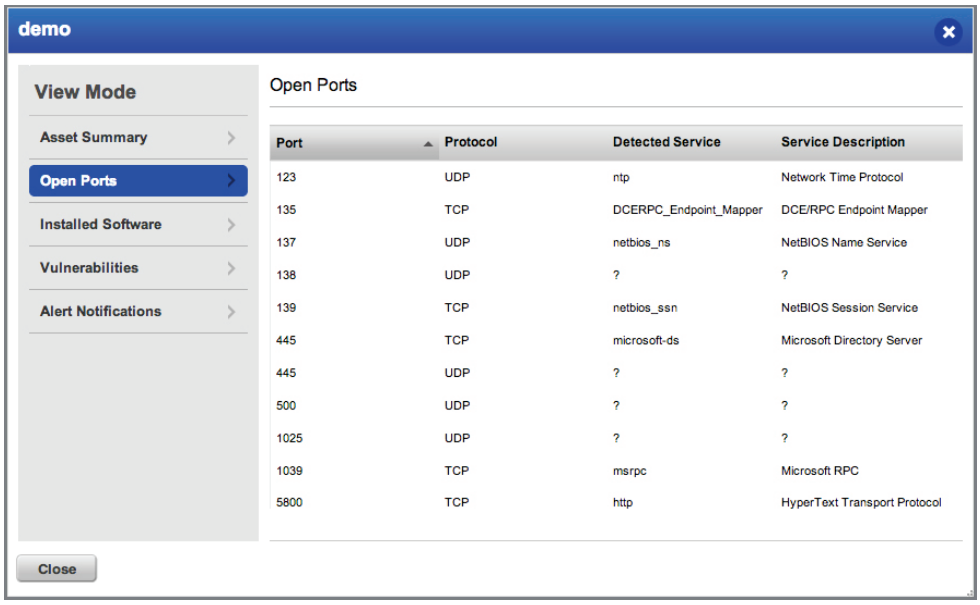


Figure 1: Qualys Continuous Monitoring shows all open ports, protocols and related services on every host.

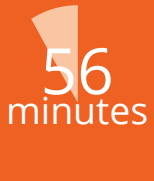
TIME BOMB

The continuous flood of new vulnerabilities coupled with constant changes to your IT environment means the fuse will always be short with little time to fix high priority assets.

For hosts attached to the Internet with open ports and services:

Average time to 1st scan

Average time to 1st vulnerability scan



Average time to 1st exploit

Source: "How Vulnerable are Unprotected Machines on the Internet?" (Study by the University of Michigan, 2014)

“In an era of continuous compromise, **enterprises need to shift** from a mindset of “incident response” – wherein incidents are thought of as occasional, one-off events – **to a mindset of continuous response** – wherein attacks are relentless, hackers’ ability to penetrate systems and information is never fully blocked, and systems must be assumed to be continuously compromised, and this, they must be **continuously monitored**,”

said **Neil MacDonald,** Vice President and Distinguished Analyst for Gartner.

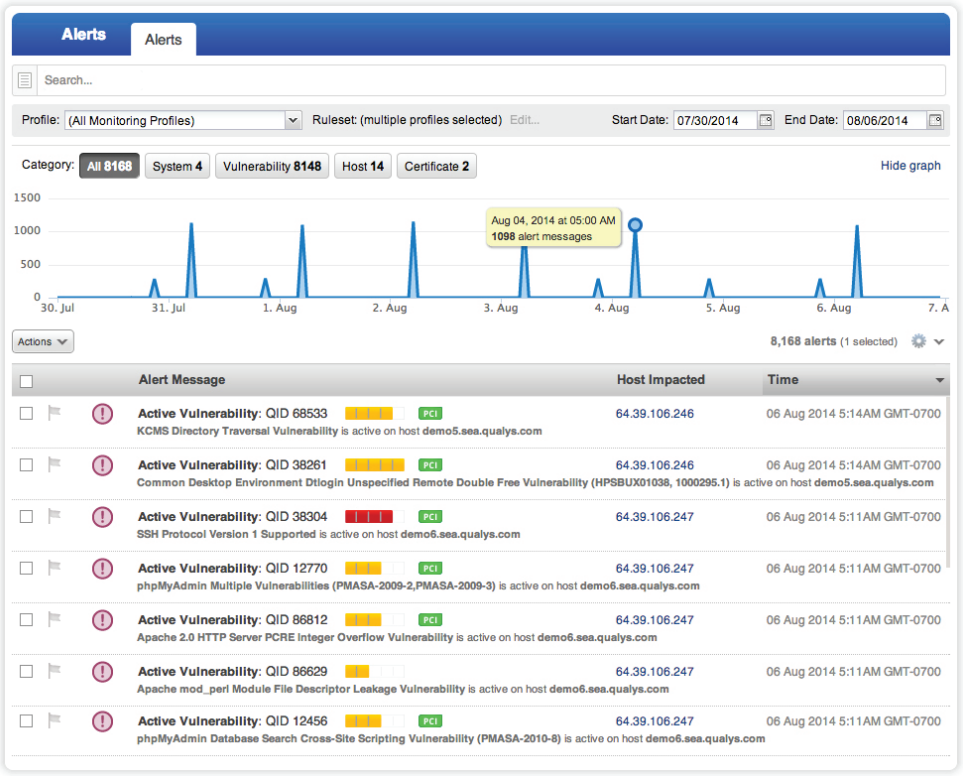


Figure 2: Qualys Continuous Monitoring alerts let first responders instantly drill down to details such as new open ports, port closed, or port changed.

Who is notified by CM and how often. A policy engine in Qualys CM is configured to ensure that notifications go to specific first responders on operations teams who are responsible for associated priority assets requiring remediation.

In conjunction with designating who should receive specific alerts, Qualys CM offers eight standard intervals for event notification. The first two, “every 5 minutes” and “every 20 minutes” are for the most critical events and are the ones you should use for true “continuous monitoring.” For example, if a first responder is designated to receive alerts every five minutes, that person will receive all priority-designated alerts that have occurred in the prior five minute interval. Clumping transmission of alerts into intervals of five or 20 minutes helps to minimize email or pager spam while keeping notification timely.

Longer intervals such as every 12 hours, once a day or once a week are appropriate for lower priority events and may be used for staffers tasked with handling those tasks.

Alerts may also be sent to people who are not authorized users of Qualys services. For example, a Security Operations Center analyst might not be directly involved with remediation, but should be aware of urgent vulnerabilities that could affect the network.

SIEM Integration for Enterprise Systems. A new extensible API incorporates Qualys CM alerts into enterprise incident response systems via integrations with leading platforms for Security Information and Event Management (SIEM), including Splunk and HP ArcSight. Qualys CM uses the Common Event Format (CEF) to send events into all popular SIEM and incident response products – including email alerts directly to the inbox of first responders.

EXAMPLES OF RESULTS USING QUALYS CM

Alerts sent by Qualys CM to first responders specify changes in an organization's attack surface that may result in a compromise of asset security. Examples of typical significant events include:

- **New vulnerability found** – Alerts are sent based on severity level of the vulnerability and the affected host. You can also specify alerts for specific vulnerabilities. For example, even though patches were published for the infamous Heartbleed Bug, this vulnerability continues to appear due to deployment of hosts infected by bad images used for configuration. Specifying a rule that searches for "QID 42220" will immediately identify the presence of this vulnerability, and Qualys CM will notify first responders accordingly.
- **New host** – Appearance of a new host on our network is a significant event. For example, you could specify a rule permitting hosts in the DMZ to only run Linux, and only have port 80 and port 443 open, plus port 22 for remote management. Qualys CM will immediately detect hosts with variations from the rule and notify first responders accordingly.
- **New open port** – A host may have been securely configured in the past, but if a port is deliberately or accidentally opened, this is an event that exposes the machine to attack. Qualys CM notes this event and alerts first responders accordingly. Rules specified with Qualys CM can monitor granular port-related criteria such as hosts not running Windows with port 80 open.
- **New software installed** – Qualys CM can send an alert if a host has new software installed (including an upgrade or downgrade), or is running a version of software that is out-of-date and/

LEARN MORE

Learn more about Qualys Continuous Monitoring. This solution is part of the Qualys Cloud Platform, and is sold as an annual subscription with Qualys Vulnerability Management. For more information and a free 7-day trial, please visit https://qualys.com/cm-trial

or unpatched. This capability is enabled by configuring Qualys Vulnerability Management to do authenticated scanning, which logs the scanner into the host as if it were an authorized user of the machine.

- **Changes in a SSL certificate** – Usually these alerts are related to multiple hosts. Granular alert criteria may include certificates that are new (even though they may be valid and not expired). This event is important because it detects when someone may have swapped in a valid certificate, but not the certificate that should be used for a particular host. For example, if your organization only buys certificates from Verisign, a rule specifying that will automatically detect an invalid certificate purchased elsewhere, such as from GoDaddy.

Rule Sets such as those governing results described above can be re-used as often as you like, thus simplifying administration and use of Qualys CM.

Finally, a new all-in-one Guided Search Box feature in Qualys CM helps users to quickly locate and analyze detailed event information.

Continuous monitoring is more than a product or solution – it's a critical approach to ensure the ongoing protection of your network's perimeter. Qualys Continuous Monitoring provides an always-on, comprehensive view of your perimeter with integrated alerts so you can act quickly to address potential threats when changes occur in your network environment.

ABOUT QUALYS

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud security and compliance solutions with over 6,700 customers in more than 100 countries, including a majority of each of the Forbes Global 100 and Fortune 100. The Qualys Cloud Platform and integrated suite of solutions help organizations simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications. Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, Accuvant, BT, Dell SecureWorks, Fujitsu, NTT, Symantec, Verizon and Wipro. The company is also a founding member of the Cloud Security Alliance (CS) and. and Council on CyberSecurity. For more information, please visit **www.qualys.com.**

Qualys and the Qualys logo are proprietary trademarks of Qualys, Inc. All other products or names may be trademarks of their respective companies.

Qualys, Inc. – Headquarters
1600 Bridge Parkway
Redwood Shores, CA 94065 USA
T 1 (800) 745.4355

Qualys is global company with offices around the world.
To find an office near you, visit, **http://www.qualys.com**

© Qualys and the Qualys logo are proprietary trademarks of Qualys, Inc. All other products or names may be trademarks of their respective companies. 8/14