QUALYS® ON DEMAND SECURITY

Automating the SANS 20 Critical Security Controls with QualysGuard

The SANS 20 Critical Security Controls 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 Controls 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. Four tenets were fundamental defining the Critical Controls: 1) focus on continuous monitoring to test and evaluate remediation; 2) automate processes to address security with efficiency, reliability and scalability; 3) provide common metrics allowing all stakeholders to objectively evaluate and adjust security measures; and 4) put the organization in charge by using knowledge of actual attacks to build effective defenses. By following the guidelines of Critical Controls, your organization can ensure the confidentiality, integrity and availability of its information technology assets.

This paper describes how automating these controls with QualysGuard can protect your network and IT assets with continuous security.

CONTENTS

Background of the Critical Controls..... 1

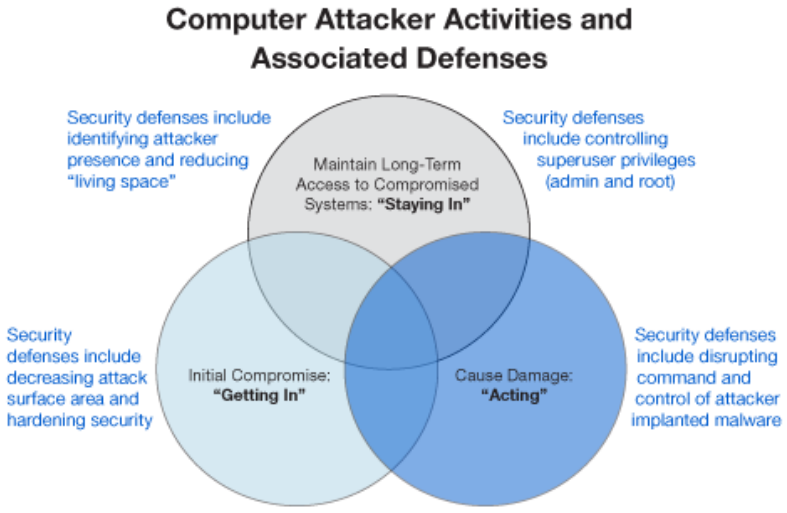
Why Critical Controls Matter to Your Organization..... 2

How QualysGuard Helps Automate Critical Controls..... 2

About QualysGuard Cloud Platform..... 8

Background of the Critical Controls

The Critical Controls started as a program called "Consensus Audit Guidelines" to improve cyber security for U.S. federal civilian agencies and the military. They are all subsets of what NIST prescribes for FISMA compliance. The Critical Controls provide a roadmap for quickly reducing security risks for three common attack strategies with four related defenses, shown in the figure below.



How Critical Controls help fight attacks (Source: SANS)

EXPERT INPUT TO CRITICAL CONTROLS

- US National Security Agency Red Team and Blue Team
- US Dept. of Homeland Security, US-CERT
- US DoD Computer Network Defense Architecture Group
- US DoD Joint Task Force: Global Network Operations (JTF-GNO)
- US DoD Defense Cyber Crime Center (DC3)
- US Dept. of Energy, Los Alamos Lab, and three other National Labs
- US Dept. of State, Office of the CISO
- US Air Force
- US Army Research Laboratory
- US Dept. of Transportation, Office of the CIO
- US Dept. of Health and Human Services, Office of the CISO
- US Government Accountability Office (GAO)
- MITRE Corporation
- The SANS Institute
- Plus commercial penetration testing and forensics experts at InGuardians and Mandiant

The Critical Controls address the most common vulnerabilities, such as open system administration channels, default and weak passwords, end-users having administrative privileges, outdated software versions, non-hardened system configurations and flaws in system administration. The Critical Controls were developed over the past decade by consensus of many federal and civilian cyber forensic experts, security experts, researchers, military experts, and federal CIOs and CISOs with intimate knowledge of cyber attacks. Among these inputs are the Associated Manageable Network Plan Milestones and Network Security Tasks developed by the National Security Agency (NSA), and the Security Content Automation Program sponsored by NIST. The Critical Controls are managed by the SANS Institute.

Why Critical Controls Matter to Your Organization

Threats to commercial and federal systems and critical infrastructure come from sovereign states, terrorists, criminals, lone hackers, and mistakes committed by staff and contractors. A successful exploit would be disastrous if it stopped vital functions of industries such as financial services or transportation, and essential functions of government and critical services. Critical Controls simplify the most urgent requirements of the NIST SP800-53 framework, which includes hundreds of technical and program management controls. Implementation of Critical Controls focuses risk reduction efforts and can lower exposure by 80 percent or more. The use of Critical Controls also can put a federal agency well on the path to compliance with FISMA – requirements that may also apply to contractors providing services to federal agencies.

How QualysGuard Helps Automate Critical Controls

The following describes how QualysGuard helps automate SANS Critical Controls. For technical details on implementation and testing of each Critical Control, click on the associated link, which connects to in-depth documents and supplemental resources on the SANS Critical Controls web site.

Critical Control 1 – Inventory of Authorized and Unauthorized Devices

Criminal hackers will attempt to breach your network through any device with an IP address. Critical Control 1 helps to mitigate this risk by providing processes and tools that identify authorized and unauthorized devices on your network. You cannot protect devices until they are first identified, so taking an accurate inventory of everything is a vital step for network security.

How QualysGuard Helps

- The QualysGuard mapping feature automatically discovers, identifies and maps all IP devices on the external network perimeter.
- For mapping all IP devices on internal networks, use a physical or virtual QualysGuard Scanner Appliance.
- The mapping feature provides details on discovered devices including IP address, machine name, operating system, and running services. (See Fig. 1 for an example.)
- QualysGuard identifies newly added and removed machines for change control through the Delta report. (See Fig. 2 for an example.) SANS Critical Control 1 mentions this capability as one of the most important for ensuring network security.

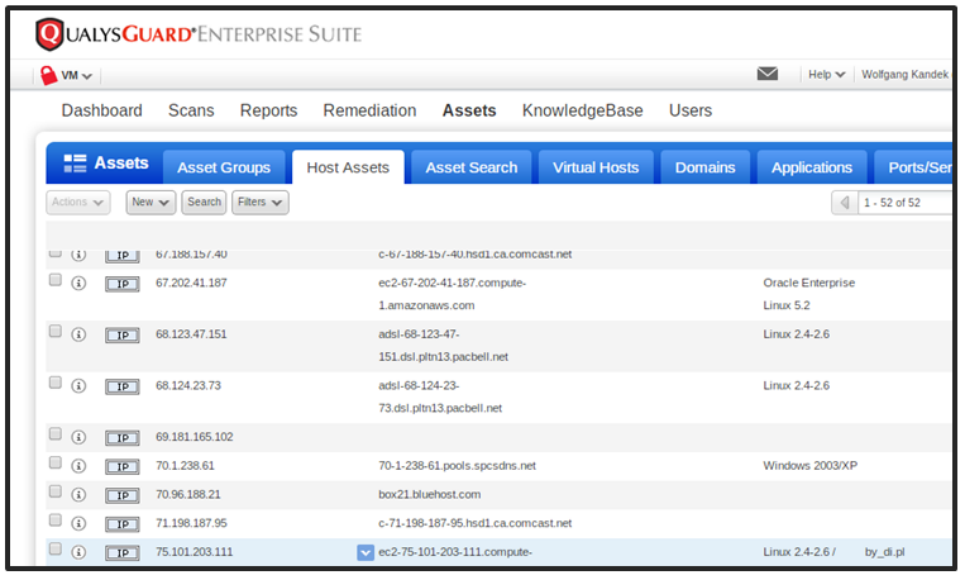


Fig. 1. QualysGuard hardware inventory report with details for each IP

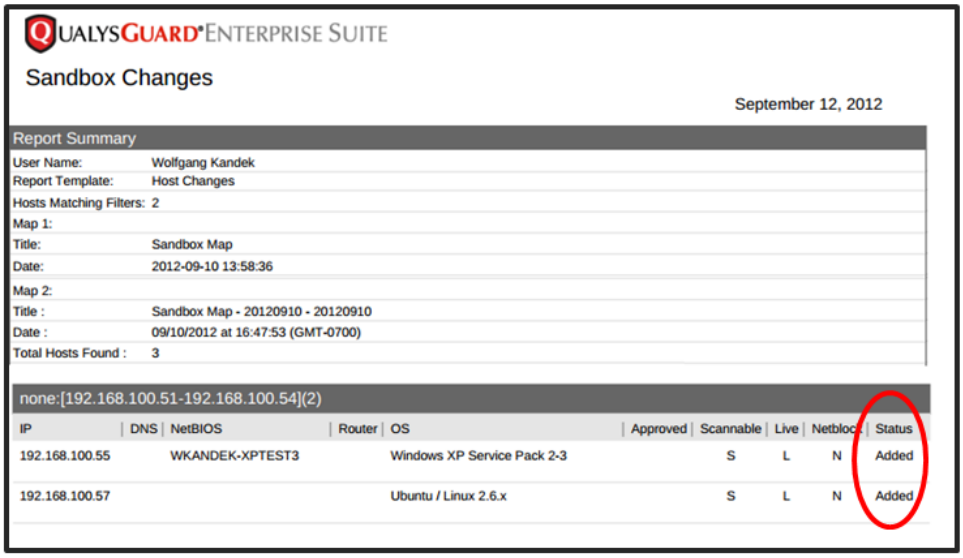


Fig. 2. QualysGuard hardware inventory Delta report

Critical Control 2 – Inventory of Authorized and Unauthorized Software

Criminal hackers will attempt to breach your network by exploiting vulnerabilities in applications on servers and workstations connected to your network. Critical Control 2 helps to mitigate this risk by providing processes and tools that identify applications on your network. You cannot protect these applications until they are first identified, so taking an accurate inventory of applications is a vital step for network security.

How QualysGuard Helps

- QualysGuard automatically discovers, identifies and builds an inventory of all software installed on scanned systems.
- QualysGuard allows interactive searching for all software in the inventory.
- QualysGuard also identifies rogue software on systems through its Blacklisting feature. (See Fig. 3 for an example.) SANS Critical Control 2 mentions this feature as vital for ensuring network security.

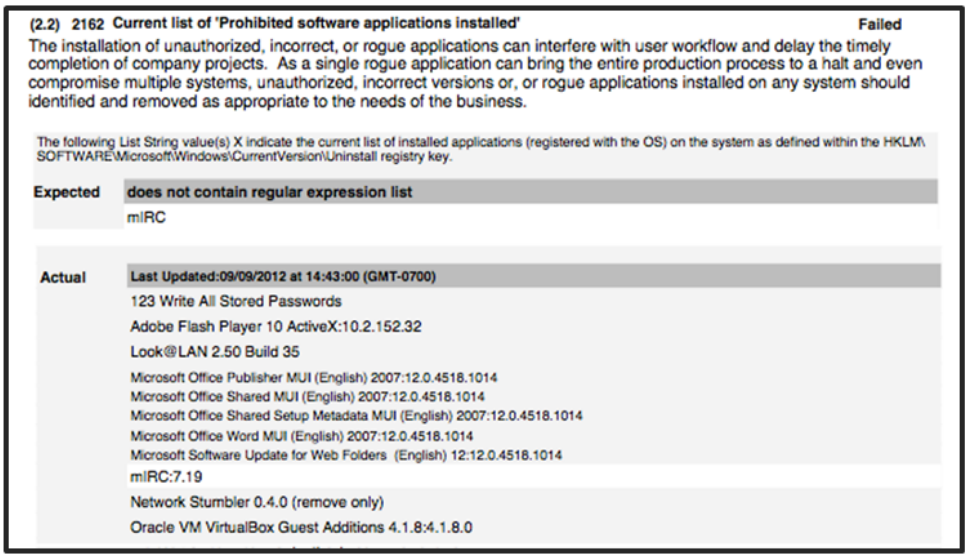


Fig. 3. QualysGuard rogue software report

Critical Control 3 – Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Known default configurations of hardware and software on mobile devices, laptops, workstations and servers are a primary vulnerability exploited by criminal hackers. The control for mitigating this risk is ongoing use of a configuration management tool that tracks configurations and changes to hardware and software on your network.

How QualysGuard Helps

- QualysGuard allows you to define secure configuration policies for the enterprise.
- It evaluates IT assets against the configuration policies to ensure compliance, and identifies all deviations from policy.
- The solution supports enterprise frameworks including CIS, COBIT, ISO, and NIST.
- Qualys also provides a Certified SCAP FDCC Scanner, Authenticated Configuration Scanner, Authenticated Vulnerability and Patch Scanner, Unauthenticated Vulnerability Scanner and Vulnerability Database.

Critical Control 4 – Continuous Vulnerability Assessment and Remediation

New vulnerabilities in software for devices and applications are discovered every day. Criminal hackers seek to exploit these and gain access to your network. It's vital that your organization perform continuous vulnerability assessments to identify weak points – and remediate them quickly in order of their strategic priority of enterprise functions on the corresponding assets. Your organization will achieve efficiency and accuracy in these tasks by using processes and tools that evaluate known vulnerabilities against configurations of all devices and software contained in the enterprise network inventory database.

How QualysGuard Helps

- QualysGuard scans periodically (by schedule) for vulnerabilities on all network-connected systems.
- QualysGuard also provides scans on demand for ad hoc checks, or for specific vulnerabilities. See Fig. 4 for a sample report showing results of a scan for "forbidden ports," which is recommended by SANS Critical Control 4.
- The solution also supports continuous scanning for mission-critical systems and sub-networks.

PRIORITZING YOUR SECURITY EFFORTS

SANS Critical Controls prioritize the most important steps first for quickly reducing risk of successful exploits.

Effect on attack mitigation:

- *Very High:* Critical Controls 1–4
- *High:* 5–7
- *Moderately High to High:* 8–9
- *Moderately High:* 10–11
- *Moderate to Moderately High:* 12
- *Moderate:* 13–16
- *Moderately Low to Moderate:* 17–18
- *Low:* 19–20

- QualysGuard 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.

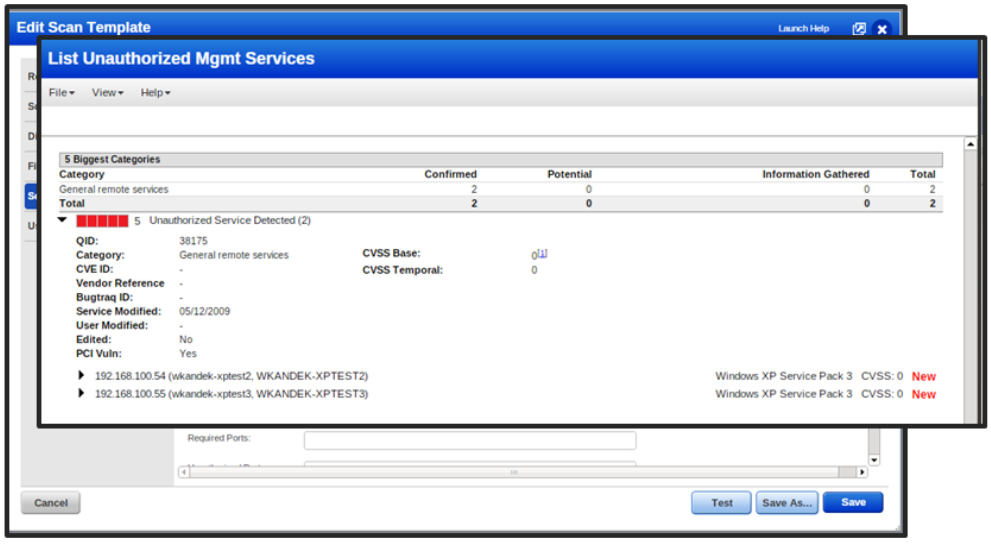


Fig. 4. QualysGuard report showing results of a scan for forbidden ports

Critical Control 5 – Malware Defenses

Malicious software is a major vector exploited by criminal hackers. Critical Control 5 entails processes and tools used to detect, prevent and correct installation and execution of malicious software on all devices connected to the network.

How QualysGuard Helps

- QualysGuard verifies deployment of third party anti-virus, spam and anti-malware software, and for configuration policy exceptions.
- The solution scans your enterprise web sites for malware.
- QualysGuard integrates with third party NAC solutions to enforce updates to endpoint devices of the most recent security software prior to granting network access.

Critical Control 6 – Application Software Security

Vulnerabilities in web-based and other application software are a major vector of exploitation by criminal hackers. Critical Control 6 prescribes processes and tools for detecting, preventing and correcting security weaknesses during the development and acquisition of software applications.

How QualysGuard Helps

- QualysGuard WAS builds an inventory of all web applications on the network.
- The solution scans web applications for known vulnerabilities, such as those using SQL injection and cross-site scripting.
- It also verifies database hardening measures.
- QualysGuard WAS supports the Open Web Application Security Project (OWASP) Top 10 Project.

Critical Control 7 – Wireless Device Control

Wireless devices are a growing threat to network security, particularly as employees use potentially at-risk personal devices to access enterprise resources. Wireless also enables attacks from outside the organization's physical buildings by connecting via Wi-Fi access

points inside the organization. This control encourages the use of processes and tools that identify, track and remediate these vulnerabilities.

How QualysGuard Helps

- QualysGuard identifies authorized and rogue wireless access devices on the network.

Critical Control 8 – Data Recovery Ability

This control is for ensuring the use of data backup and recovery processes and tools that protect an organization from attacks through machines that may have been compromised.

How QualysGuard Helps

Not applicable.

Critical Control 9 – Security Skills Assessment and Appropriate Training to Fill Gaps

Attackers may attempt to breach a network by exploiting weaknesses in an enterprise workforce. This control addresses related gaps in skills and training.

How QualysGuard Helps

Not applicable.

Critical Control 10 – Secure Configuration for Network Devices such as Firewalls, Routers, and Switches

The prototypical attack is exploitation of vulnerabilities in devices on the network perimeter, such as firewalls, routers and switches. Critical Control 10 helps to identify and remediate security weaknesses in the configurations of these network devices based on formal configuration management and change control tools and processes.

How QualysGuard Helps

- QualysGuard verifies best practice settings on firewalls, routers and switches.
- As a baseline, QualysGuard allows network administrators to define secure configuration policies for perimeter devices.
- QualysGuard scans automatically evaluate IT assets against configuration policy.
- The solution also identifies all deviations from policy to facilitate remediation.

Critical Control 11 – Limitation and Control of Network Ports, Protocols, and Services

Vulnerabilities in remotely accessible network services are pursued by attackers who scan for opportunities to try default user IDs and passwords or widely available exploitation code. This control entails processes and tools that track, control, prevent and remediate the use of ports, protocols and services on networked devices.

How QualysGuard Helps

- QualysGuard identifies open TCP/UDP ports on scanned systems.
- The solution identifies services running on non-standard ports.
- QualysGuard also discovers policy violations of potentially vulnerable services by comparing them against customer-defined allowed vs. prohibited lists.

Critical Control 12 – Controlled Use of Administrative Privileges

A primary attack vector is the misuse of administrator privileges. An exploit might trick a workstation user running as a privileged user, or by guessing or cracking an administrator's password. Either way, unauthorized administrative access can lead to a catastrophic breach of network security. Critical Control 12 provides processes and tools

to track, control, prevent, and correct the use, assignment and configuration of administrative privileges on computers, networks and applications.

How QualysGuard Helps

- QualysGuard validates password requirements on systems.
- The solution lists users with administrative privileges on all systems.

Critical Control 13 – Boundary Defense

This control provides processes and tools that help detect, prevent and correct the flow of information transferring networks of different trust levels, focusing on security-damaging data.

How QualysGuard Helps

Not applicable.

Critical Control 14 – Maintenance, Monitoring, and Analysis of Audit Logs

This control provides the means to detect, prevent and correct the use of systems and information based on audit logs of events that are considered significant or could impact the security of an organization.

How QualysGuard Helps

- QualysGuard can validate audit log settings on Windows systems.

Critical Control 15 – Controlled Access Based on the Need to Know

"Need to know" is a classic enterprise security policy. The presence of uncontrolled access to all or most information on a network makes it easy for attackers to exfiltrate important data once they gain access. This control tracks and controls access based on which users, computers, and applications have authorized access based on an approved classification.

How QualysGuard Helps

- QualysGuard tests file permission and custom Windows registry checks against policy to identify unauthenticated file and share access.
- The solution enumerates users, groups and system account and associated privilege levels.

Critical Control 16 – Account Monitoring and Control

Inactive user accounts are subject to exploit by attackers who use them to gain access to a network and its resources. Since these accounts are legitimate, it's difficult for network watchers to track nefarious activity. This control implements processes and tools to track, prevent and remediate the use of system and application accounts.

How QualysGuard Helps

- QualysGuard provides visibility into configuration of systems.
- The solution compares deployed configurations against policy and identifies systems that are non-compliant.

Critical Control 17 – Data Loss Prevention

Data Loss Prevention (DLP) is the use of policy-based processes and tools that track, control, prevent and correct data transmission and storage. Policy is based on the data's content and associated "right to know" classification. DLP is usually associated with keeping sensitive data inside an organization and preventing its accidental or deliberate exfiltration.

How QualysGuard Helps

- QualysGuard evaluates configuration settings for all Windows-based systems on the network, including removable media such as USB, CD-ROM and floppy drives.
- QualysGuard WAS evaluates all web pages for the presence of inappropriate or sensitive data.

Critical Control 18 – Incident Response and Management

Organizations need to have a properly tested plan in place for directing trained resources to deal with adverse events or threats of adverse events. This control includes one or more sub-controls requiring manual validation of an Incident Response and Management plan.

How QualysGuard Helps

Not applicable.

Critical Control 19 – Secure Network Engineering

This control is intended to be pre-emptive, providing processes and tools to build, update and validate a network infrastructure that can withstand attacks from advanced threats. It includes one or more sub-controls requiring manual validation.

How QualysGuard Helps

Not applicable.

Critical Control 20 – Penetration Tests and Red Team Exercises

Penetration tests and Red Team exercises simulate attacks on a network. They are used to validate the security posture of an organization. This control includes one or more sub-controls requiring manual validation.

How QualysGuard Helps

- QualysGuard provides vulnerability data as input to penetration testing tools.

LEARN MORE

Learn more about how the QualysGuard Cloud Suite can quickly automate Critical Controls by helping your organization to discover, catalog, scan and control these risks with a scalable cloud solution. For details, contact your Qualys sales representative and visit http://www.qualys.com/enterprises/qualysguard/.

About QualysGuard Cloud Platform

The QualysGuard Cloud Platform and its integrated suite of security and compliance applications helps provide organizations of all sizes with a global view of their security and compliance posture, while reducing their total cost of ownership. The QualysGuard Cloud Suite, which includes Vulnerability Management, Web Application Scanning, Malware Detection Service, Policy Compliance, PCI Compliance and Qualys SECURE seal, enable customers to identify their IT assets, collect and analyze large amounts of IT security data, discover and prioritize vulnerabilities and malware, recommend remediation actions an verify the implementation of such actions. The platform's applications and services are used today by more than 6,000 organizations in more than 100 countries, including a majority of each of the Forbes Global 100 and Fortune 100.

QUALYS® ON DEMAND SECURITY

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**