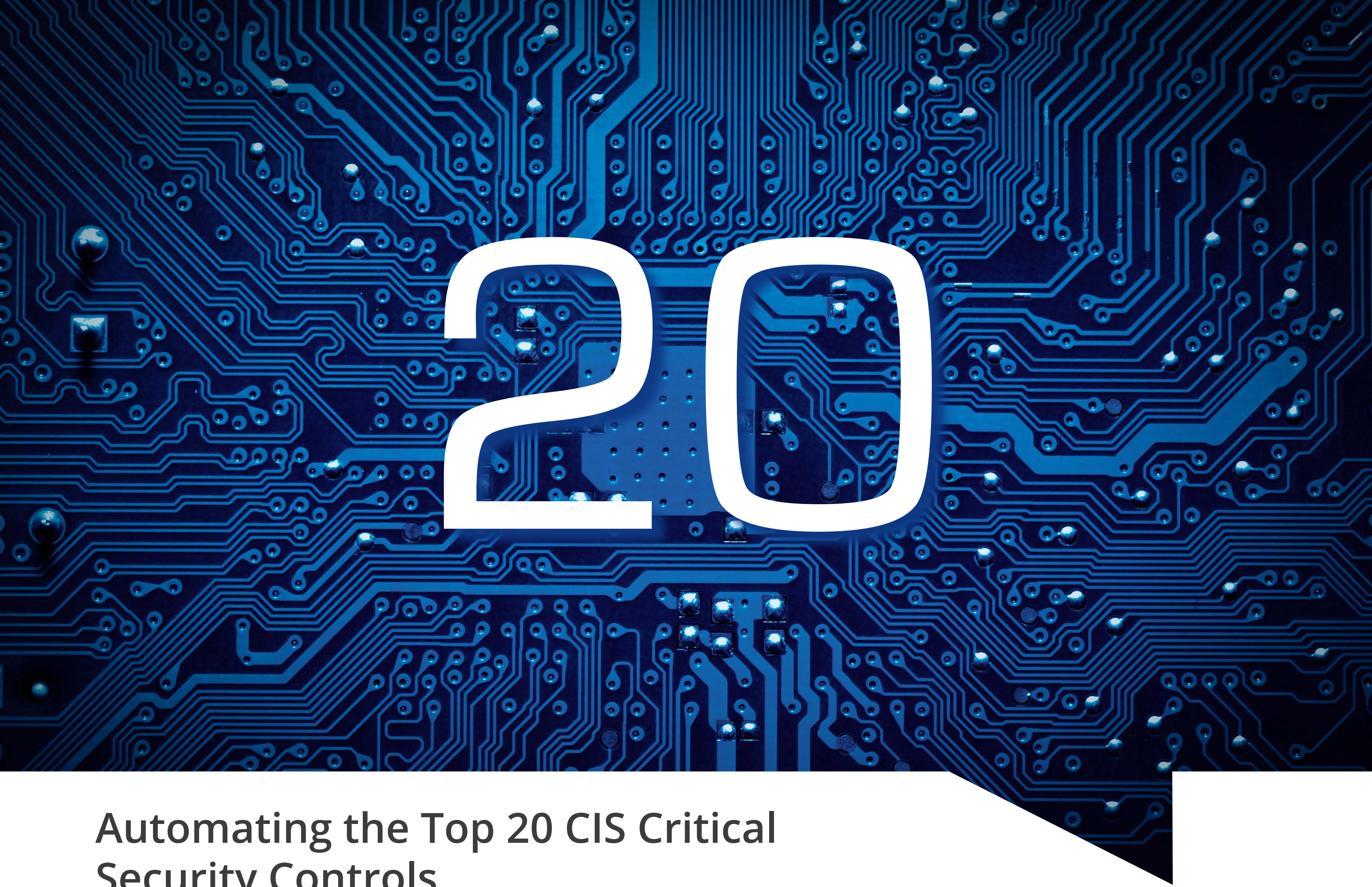


Automating the Top 20 CIS Critical Security Controls

QUALYS®

SUMMARY

It’s not easy being today’s CISO or CIO. With the advent of cloud computing, Shadow IT, and mobility, the risk surface area for enterprises has increased dramatically, while IT budgets have shrunk and skilled cyber security talent is virtually impossible to find.

Thankfully, the CIS Top 20 Critical Controls provides a pragmatic approach, offering prioritized guidance on the important steps for implementing basic cyber hygiene practices. With the CIS Top 20 Critical Security Controls, CISOs now have a blueprint for reducing risk and managing compliance.

By automating each of these controls, CISOs enable their information security teams to do much more with less, essentially operationalizing good cyber hygiene.

BACKGROUND: A BLUEPRINT FOR CYBER SECURITY

Led by the Center for Internet Security (CIS) and in coordination with the SANS Institute, the Critical Security 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. Representing the culmination of close collaboration, community and consensus, the CIS Top 20 Critical Security Controls enable a prioritized, risk-based approach to cyber security. Cyber security professionals from across the private and public sector came together to answer these important questions:

“In practice, what works and where do you start?”

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such as open system administration channels, default and weak passwords, end-users having administrative privileges, outdated software versions, non-hardened system configurations and flaws in system administration.

KEY CYBER SECURITY SUCCESS FACTORS

The Achilles heel for many information security professionals lies in their desire for perfection at the expense of pragmatism. The uncomfortable reality is that no security control will ever be perfect, and so it's best to focus on those controls that have the biggest impact in reducing risk while optimizing efficiency. It's even more critical to establish an automated approach for implementing and measuring these controls for continuous security and compliance.

AUTOMATE THE CRITICAL SECURITY CONTROLS (CSC)

As a critical tenet for the CSCs, automation provides a key role in achieving reliability, scalability and continuous security. This emphasis aligns well with Qualys' continuous security and compliance delivery model. Because the Qualys Cloud Platform offers a set of extensible services, organizations can achieve rapid implementation of the majority of the controls with a single solution. Additionally, Qualys solutions can be deployed from the cloud within a matter of hours, without costly Professional Services or any additional software or hardware requirements.

The **FIVE CRITICAL TENETS**[1] of effective cyber security

Offense Informs Defense

Use knowledge of actual attacks that have compromised systems to continually learn from these events to build effective, practical defenses. Include only those controls that can be shown to stop known real-world attacks.

Prioritization

Invest first in controls that will provide the greatest risk reduction and protection against the most dangerous threat actors and that can be feasibly implemented in your computing environment.

Metrics

Establish common metrics to provide a shared language for executives, IT specialists, auditors, and security officials to measure the effectiveness of security measures within an organization so that required adjustments can be identified and implemented quickly.

Continuous Diagnostics and Mitigation

Carry out continuous measurement to test and validate the effectiveness of current security measures and to help drive the priority of next steps.

Automation

Automate defenses so that organizations can achieve reliable, scalable, and continuous measurements of their adherence to the controls and related metrics.

[1] **Source:** http://www.cisecurity.org/critical-controls.cfm

CRITICAL SECURITY CONTROL

HOW QUALYS HELPS

1 INVENTORY OF AUTHORIZED & UNAUTHORIZED DEVICES

Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

With Qualys' Cloud Agent and AssetView service, you'll have a continuously updated inventory of all assets, including detailed hardware information (e.g. installed RAM, Mac Addresses, Firmware, and more).

Additionally, installing Qualys Scanner Appliances on your internal networks enables discovery of newly added devices that may be unauthorized or unmanaged, and then tag these for follow up and remediation.

2 INVENTORY OF AUTHORIZED & UNAUTHORIZED SOFTWARE

Actively manage (inventory, track, and correct) all software on the network Vso that only authorized software is installed and can execute, and that and unauthorized and unmanaged software is found and prevented from installation or execution.

With Qualys' Cloud Agent and AssetView service, you'll have a continuously updated inventory of all software assets, including details on what software is running on which machines, in order to flag unauthorized or unmanaged software for removal.

Furthermore, you can run quick searches to identify unauthorized software across all your assets, and then convert these into dynamically generated dashboards, alerts, and reports.

3 SECURE CONFIGURATIONS FOR HARDWARE & SOFTWARE ON MOBILE DEVICES, LAPTOPS, WORKSTATIONS & SERVERS

Establish, implement, and actively manage (track, report, correct) the security configuration of laptops, servers and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

Qualys' Policy Compliance evaluates IT assets against secure configuration policies to identify gaps in coverage, policy violations and other risks.

In addition to the CIS Critical Security Controls, these policy checklists include support for enterprise frameworks such as COBIT, ISO, and NIST as well as regulatory standards such as PCI DSS, HIPAA, and SOX.

Qualys also provides a Certified SCAP FDCC Scanner and Authenticated Configuration Scanner in order to track, report, and correct the security configuration of laptops and servers across your enterprise.

CRITICAL SECURITY CONTROL

HOW QUALYS HELPS

4 CONTINUOUS VULNERABILITY ASSESSMENT & REMEDIATION

Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

With a Six Sigma Accuracy level of 99.99%+, Qualys' Vulnerability Management and Continuous Monitoring enables you to continuously identify vulnerabilities and react with confidence and focus.

Offering vulnerability scanning for internal networks, external networks, cloud environments and more, Qualys gives you a unified picture of your overall risk surface area, so that you can prioritize and focus your defenses.

5 CONTROLLED USE OF ADMINISTRATIVE PRIVILEGES

The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

Qualys can track users with administrative privileges on all systems as well as assess secure configurations for system administration access (e.g. validation of password requirements).

6 MAINTENANCE, MONITORING, & ANALYSIS OF AUDIT LOGS

Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

In addition to validating audit log settings on Windows systems, Qualys offers APIs for integration with log management and SIEM systems. With this level of integration, Qualys customers can correlate vulnerability data with log data for unified security and compliance monitoring.

CRITICAL SECURITY CONTROL

HOW QUALYS HELPS

7 EMAIL & WEB BROWSER PROTECTIONS

Minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems.

Qualys' Cloud Agents can assess and validate the installation and secure configuration of authorized web browsers, and identify and alert on the presence of insecure or authorized web browsers and email clients.

8 MALWARE DEFENSES

Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and correction action.

Qualys verifies the installation of third party anti-virus, spam and anti-malware software across your endpoints.

Additionally, Qualys' Web Application Scanning and Malware Defense Services will identify and discover web app vulnerabilities as well as the presence of hidden malware lurking on your websites.

9 LIMITATION & CONTROL OF NETWORK PORTS, PROTOCOLS AND SERVICES

Manage (track, control, correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.

Qualys identifies open TCP/UDP ports on scanned systems as well as services running on non-standard ports.

Qualys can also discover potentially vulnerable services by comparing them against customer-defined and allowed services vs. prohibited lists or blacklists.

CRITICAL SECURITY CONTROL	HOW QUALYS HELPS
10 DATA RECOVERY CAPABILITY The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.	Not applicable.
11 SECURE CONFIGURATIONS FOR NETWORK DEVICES SUCH AS FIREWALLS, ROUTERS, & SWITCHES Establish, implement and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.	Qualys' Vulnerability Management and Policy Compliance assess and verify the secure configuration of network infrastructure including proxy servers, firewalls, routers and switches. To facilitate remediation, Qualys identifies, documents, and alerts on all deviations from corporate policy.
12 BOUNDARY DEFENSE Detect, prevent, correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.	Qualys Vulnerability Management and Continuous Monitoring identifies threats and monitors unexpected changes in your boundary defenses before they turn into breaches. With this servicet, you can track what happens within your internal environment as well as the Internet-facing devices throughout your DMZs and cloud environments.

CRITICAL SECURITY CONTROL

HOW QUALYS HELPS

13 DATA PROTECTION

The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

Qualys evaluates configuration settings for all Windows-based systems on the network, including removable media such as USB, CD-ROM and floppy drives.

Additionally, Qualys Web Application Scanning evaluates all web pages for the presence of inappropriate or sensitive data.

14 CONTROLLED ACCESS BASED ON THE NEED TO KNOW

The processes and tools used to track, control, prevent, correct security access to critical assets (e.g. information, resources, systems), according to the formal determination of which persons, computers, and applications have a need and a right to access these critical assets based on an approved classification.

With Qualys' Cloud Agents and AssetView service, you can classify and group assets based on their criticality to the business, as well as their relative risk rankings. Additionally, Qualys tests file permission and custom Windows registry checks against policy to identify unauthenticated file and share access.

As you segment your network based on the need to know, you can rely on Qualys to assess and validate that the VLAN ACLs reflect your intentions.

15 WIRELESS ACCESS CONTROL

The processes and tools used to track, control, prevent, and correct the security use of wireless local area networks (LANs), access points, and wireless client systems.

Qualys can discover rogue wireless access points, and assess the security configurations of these devices to prevent data exfiltration.

CRITICAL SECURITY CONTROL

HOW QUALYS HELPS

16 ACCOUNT MONITORING & CONTROL

Actively manage the life cycle of system and application accounts – their creation, use, dormancy, deletion – in order to minimize opportunities for attackers to leverage them.

Qualys provides visibility into the configuration of systems, which includes the creation, use and deletion of system and application accounts. In assessing systems against the required secure configurations, Qualys identifies and flags systems that are out of compliance with this critical control.

17 SECURITY SKILLS ASSESSMENT & APPROPRIATE TRAINING TO FILL GAPS

For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training and awareness programs.

While Qualys doesn't provide security awareness training programs per se, we do offer free product training for all of our customers, and for all of our products.

Additionally, you can use Qualys' automated Questionnaire Service to assess, measure, and report on your end users' comprehension of security awareness education and training.

18 APPLICATION SOFTWARE SECURITY

Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.

Qualys' Web Application Scanning creates an automated inventory of all web applications in your environment (internal, external, virtual, and cloud-based). Additionally, it scans your web applications for known vulnerabilities (e.g. SQL injection, cross-site scripting). With our Malware Defense Service, you can also discover and alert on the presence of malware on any of your web applications.

CRITICAL SECURITY CONTROL

HOW QUALYS HELPS

19 INCIDENT RESPONSE & MANAGEMENT

Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g. plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

Not applicable.

20 PENETRATION TESTS & RED TEAM EXERCISES

Test the overall strength of an organization's defenses (the technology, the processes, and the people) by simulating the objectives and the actions of an attacker.

Qualys offers the necessary Reconnaissance tools and vulnerability data that provide the foundation for all Penetration Testing exercises and procedures. Additionally, Qualys Web Application Scanning supports a tight integration with Burp Suite to coordinate and correlate data collected from various attack discovery methods.

ABOUT QUALYS

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions with over 8,000 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. 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.

CRITICAL SECURITY CONTROLS POWERED BY THE CLOUD

With users accessing apps, data, and services across private and public clouds, now is the best time to look to cloud-based security services to provide an essential level of continuous security.

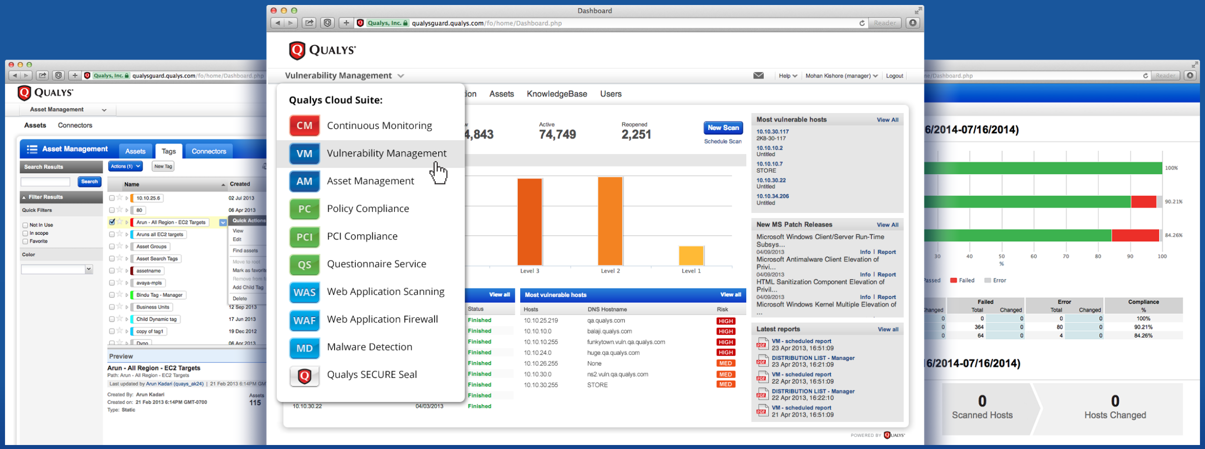
Built in and designed for the cloud, Qualys' unified suite of security and compliance services offer organizations the fastest and most efficient way to automate the broadest set of critical security controls, with particular emphasis on the top five. With our Cloud Agent and AssetView service, organizations gain real-time visibility into software and hardware inventories, what software is running, as well as whether system configurations are secure. Organizations can search for granular details about any asset attributes, and receive instant results – whether or not the asset is on-prem or in the cloud or currently offline.

Delivered on the Qualys' Cloud Platform, our integrated suite of extensible services offers rich correlation capabilities to provide the full context you need for understanding potential risks to the security and compliance of your assets. For example, vulnerability scan results, secure configuration assessments, and other data enrich the asset data we collect through our Cloud Agent and display via AssetView.

Whether implementing and automating the Top 20 critical security controls, or simply reducing risk across your organization, Qualys offers the integrated scalability you need to protect critical assets – no matter where they live or where they might roam.

Qualys extensible services include:

- AssetView Inventory Service
- Vulnerability Management and Continuous Monitoring
- Policy Compliance
- Questionnaire Service
- PCI Compliance
- Web Application Scanning
- Web Application Firewall
- Malware Detection Service
- Secure Seal


Dashboard
QUALYS
Vulnerability Management
Qualys Cloud Suite:
CM Continuous Monitoring
VM Vulnerability Management
AM Asset Management
PC Policy Compliance
PCI PCI Compliance
QS Questionnaire Service
WAS Web Application Scanning
WAF Web Application Firewall
MD Malware Detection
Qualys SECURE Seal
Asset Management
Assets
Connectors
Tags
Most vulnerable hosts
New MS Patch Releases
Latest reports
74,749
2,251
New Scan
0 Scanned Hosts
0 Hosts Changed