NARROWING THE SECURITY GAP WITH AUTOMATED CONFIGURATION ASSESSMENT

QUALYS®

CONTINUOUS SECURITY

A flood of recent breaches has pushed security and compliance professionals into urgent defense mode as they grapple with targeted multi-staged attacks, mobile threats, zero-day defects and other vulnerabilities. In looking outward for danger and potential threats, however, some security professionals have missed a key internal enabler of successful breaches: incorrect configuration of IT resources. **HP's Cyber Risk Report 2013 found 80% of applications contain vulnerabilities exposed by incorrect configuration.** By preventing exposures, organizations can make enormous strides in IT security and prevent the efforts of criminals to steal data. **In this guide, Qualys describes internal risks to IT security and three best practices to control incorrect configurations. Critical components to this include automation of assessments and prioritization of risks. By using the automation technology in Qualys Policy Compliance, organizations can ensure the safety of sensitive data and IT while meeting mandates for compliance.**

FACING THE CHALLENGES OF INSECURITY

Programming mistakes cause the most vulnerabilities in software. Correcting these is accomplished by installing vendor-supplied patches to the affected software. But careless programmers aren't the only source of vulnerabilities. The Cyber Risk Report 2013 by Hewlett-Packard Co. found that 80% of applications contain vulnerabilities exposed by incorrect configuration. Examples include failure to change default passwords, improper access control settings, undeleted example configurations, unnecessary services, weak/improper encryption configuration, or insecure deployment of an application. For example, many applications require a prerequisite installation of Internet Information Services (IIS) for Microsoft Windows Server. Often these installations are improperly configured, which makes them easy prey for attackers. When the application owner simply accepts the installation step, it establishes a fully functioning, wide open webserver on the server.

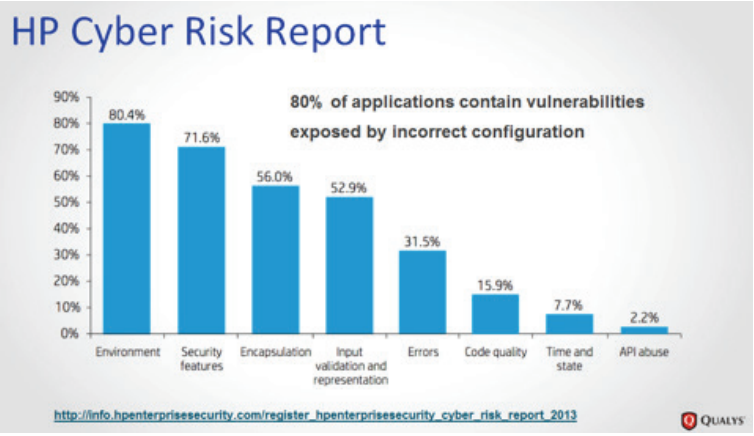

Figure 1. Incorrect configurations are a major source of risks

Controlling risks in a dynamically changing environment is daunting. This is particularly true with the "vanishing network perimeter." The edge of an organization's network used to have a clear boundary because all connections to external networks were strictly controlled by firewalls. Applying access security controls to network traffic through routers, switches firewalls was straightforward. This traditional perimeter is swiftly changing with the influx of mobile devices, remote access by employees, contractors and partners; plus programs such as Bring Your Own Device (BYOD) – all of which multiply paths to the Internet that are outside the direct supervision of an organization's access security controls. Distinguishing "good guys" from "bad guys" is now far more difficult.

Virtualization and adoption of cloud-based technologies further challenge our ability to secure the environment. Sometimes employees sneak these technologies into use in order to circumvent restrictions of the IT department. Unfortunately for security, you can't defend what you aren't aware of. And even if you are, sanctioned virtualized assets might not be powered on during assessment. The cloud promises endless scalability on demand, so dormant assets or systems only online for minutes at a time will become commonplace. These assets can harbor undetected misconfigurations that evade detection and persist within the IT environment.

Strong and consistent configuration standards are mandatory to reduce these risks, and organizations should strive to implement automated configuration assessment to provide the metrics needed to enforce policy. Quite often the validation of security requirements is manual, so policy enforcement can't keep pace with the constant change in IT. Infrequent assessment and unclear prioritization result in the widening misconfiguration gap that plagues many organizations. The next section presents three best practices to narrow this gap and improve security posture.

BEST PRACTICES FOR EFFECTIVE POLICY ENFORCEMENT

A systematic program for IT security will include several goals. Primary objectives are to reduce risk exposure, demonstrate due diligence, and to enforce compliance with policy. Here are three best practices for accomplishing these goals.

1 Establish & Implement Controls

Effective controls are critical to enforcing IT security policy and meeting regulatory requirements. With a vast array of mandates impacting organizations today, selecting the right controls can be a challenge. The first step is to identify mandate requirements and select a framework for guidance on identifying control objectives.

Examples of government and industry regulations include financial reporting and accountability (SOX); non-public personal information, including financial information (GLBA) and payment card data (PCI DSS); protected health information (HIPAA); energy regulation (FERC and NERC); personal information breach notification (Calif. SB1386 and ARRA); government computer security (FISMA). These sources along with internal and external; and auditors' mandates drive the overarching requirement for strong IT security controls.

Due to the complexity of multiple mandates, your organization should adopt a security control framework to make sure that all mandates and policy objectives are met. Security frameworks by government and industry organizations are where you find specific descriptions of multi-layer IT security control objectives. Focus on these to ensure you are using all the necessary controls to protect your IT environment. Auditors can help with establishing and deploying appropriate security controls using common frameworks such as:

- **COSO** – Committee of Sponsoring Organizations of the Treadway Commission
- **COBiT** – Control Objectives for Information and Related IT
- **NIST** – National Institute of Standards and Technology
- **ITIL** – Information Technology Infrastructure Library
- **FFIEC** – Federal Financial Institution Examination Council
- **CRC** – Critical Security Controls from the Council on Cybersecurity

The second step is defining technical standards for your primary IT technologies. The latter includes operating systems such as Windows and Linux, applications such as databases and web servers, and network devices such as routers, switches and firewalls. Standards consist of technical controls that enforce selected control objectives.

The easiest way to start is to let someone else do the work! Many organizations have built technical standards for all sorts of technologies. The most widely known is the CIS Security Benchmarks published by the Center for Internet Security, a consortium of industry leaders contributing to the selection and review of key security controls.

From there, you are likely to have a few gaps, and also some controls that may not work for your organization. Fine tune the benchmark to fit your organization by implementing compensating controls, adjusting the pass/fail criteria, and implementing exceptions where necessary. Add any necessary additional controls to fill remaining gaps, and then review with IT management to make sure everyone is on board.

> Qualys Policy Compliance validates that we have the controls set the way they need to be. We can see if everything is being managed as it should, or if something was changed out of the scope of policy that we would want to see right away.
>
> **John Woods**
> Director of Information Security
> PDX, Inc.

Checklist for Managing IT Policy Compliance

1. **Remember the Big Picture** – maintain your perspective, understand the auditor mentality, and prove compliance
2. **Align IT Policy Compliance** and Security with the Business
3. **Understand Your IT Environment**
4. **IT Compliance** Starts with Policy
5. **Establish Accountability**
6. **Conduct a Pre-Audit** or Readiness Assessment
7. **Centralize IT Policy** Program Management
8. **Prioritize** Remediation Activities
9. **Understand How** IT Policy Compliance Management Can Help in Other Areas
10. **Regularly Monitor** the Whole Compliance Program

2 Automate Control Assessment

Automation is mandatory to effectively assess whether your IT security controls are deployed and properly configured. Spot-checking these controls is not enough because those results will always be out of date in a changing environment. Manual assessments are also inadequate as they are manpower-intensive and do not scale. Both of these approaches are especially weak for assessing controls in virtualized environments where hundreds or thousands of virtual machines are constantly spun up and down on demand. In addition to automating the ongoing assessments of technical controls, your organization should also strive to automate assessment of procedural controls to ensure that processes are in place and performing according to policy. In cases where technical control assessment is difficult or impacts few platforms, questionnaire-based assessment can also be used to automate the manual data gathering from the systems administrators of those environments.

The automation of control assessment for IT policies improves the velocity of risk reduction and enforcement of compliance. The following areas are examples where automation is beneficial to IT security configuration compliance. All of these are difficult if not impossible to manually conduct on a continuous basis in a medium-to-large enterprise. Tools such as Qualys Policy Compliance help provide the necessary automation and integrate complex processes into an enterprise-ready solution.

Understanding the Environment

In order to conduct IT security configuration assessment, you must understand your environment. Scoping the environment includes discovery of all assets, cataloging their characteristics and maintaining a current database of the computers and devices on your network. The database must include all deployed software with respective version numbers and patch history. And, of course, the database must include the software configurations for all assets – especially IT security controls.

Scanning and Remediation

Scanning is the foundational assessment process for finding and fixing the vulnerabilities in your computer systems. A vulnerability scan gives you a snapshot of the security status of your computer systems. For IT security configuration compliance, scanning should alert you to the addition of new devices, changes to usage of ports and software to allow an analysis of the changed attack surface. A vulnerability scan that runs repeatedly on a periodic basis (say daily or weekly) allows you to track the speed of applying patches and software updates, and how your security status is improving. Critical assets should be scanned continuously. Automation will ensure that scans occur when desired, and will help determine the most effective workflow for patching and updating your configurations.

Continuous Monitoring

Continuous monitoring ensures the continuity of approved configurations for critical assets – particularly for regulatory and policy requirements. This process also should automate critical alerts to first responders to allow immediate, priority remediation of configurations affecting assets with a high priority to business operations.

Change Control

Automation can tie configuration deficiencies discovered by scanning into change control processes, especially to ensure meeting service level agreements for IT service management.

Informing Stakeholders

As previously mentioned, automating the metrics of IT security configuration compliance will provide all stakeholders with information that is relevant to their domains of responsibility within the organization.

Validate Processes

Automation will help your organization to shift the traditional focus of validating controls into a broader focus of validating critical information security processes that systemically affect enterprise-wide compliance.

3 Prioritize Measurable Results to Drive Remediation

Metrics are vital for configuration compliance because they measure the state and performance of IT security controls. If your controls are configured properly, they are more likely to perform as specified. If configurations are non-compliant, your IT security is likely to be in jeopardy. Metrics will allow your security team to prioritize remediation efforts based on the importance to your business of the particular assets at risk. Metrics should provide all stakeholders with information that is relevant to their domains of responsibility within the organization. Typical reports will include:

- **Executive Dashboard** – an at-a-glance snapshot of the entire state of compliance.
- **Trends** – to provide longitudinal views over time of how well compliance efforts are progressing (or not).
- **Management Reports** – to summarize progress in more detail for specific areas of compliance (e.g. configuration compliance for network firewalls or security of cardholder data).
- **Detailed Remediation Reports** – to inform first responders and their supervisors of current "to-do" lists for vulnerability repairs in progress; typically these will enable drill-down links to technical details such as remediation history, vendor security bulletins, recommended patches and workarounds.

Metrics should be chosen to encourage the desired result. For example, scorecards are highly effective to encourage competition between teams. Also remember that control deficiencies will occur, so measuring just on counts isn't the best approach. Instead, select a metric such as Mean Time to Remediation and categorize by control criticality.

Your control reporting should present results according to their impact or potential risk. Some controls should be mandatory across the entire environment. A subset, perhaps 20% of controls that are the most critical, could be categorized as Critical controls. The remainders should be classified into other categories such as Important, Low Priority, and Informational. Some controls, such as "world-writeable files on secured servers not providing console capabilities to end users," are relatively low risk. You should never permit blank passwords.

Similarly, assets should be organized into groups based on their operational roles. Most organizations have success with segmenting by business application, especially since multi-use servers are uncommon due to the success of virtualized compute resources. For example, all systems that are part of the online e-commerce site should be organized

together. These systems should be identified by importance – since payment processing is more critical than internal test systems for IT development.

Finally, focus your metrics and remediation based on the importance of the application and the criticality of the controls deviations. After remediating the highest risk issues, team efforts can then shift to the next set of issues, repeating until it has achieved an acceptable level of control deficiencies.

BENEFITS OF AUTOMATION

As noted by the HP Cyber Risk Report, about 80% of applications contain vulnerabilities exposed by incorrect configurations. The probability of systems deviating from compliance dramatically increases for organizations using manual audits such as once a quarter. Automating more frequent control assessments reduces the probability of deviation – and thus improves the organization's risk posture (see Figure 2).

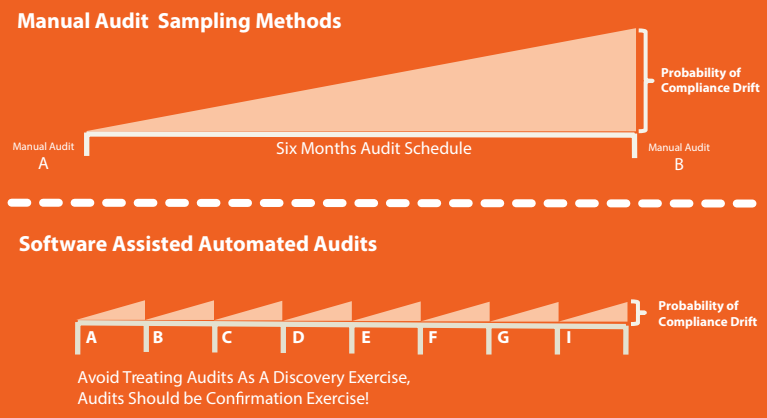

Figure 2: Probability of configuration errors declines with frequent audit

Other benefits of automation include:

- Provide a transparent, consistent and repeatable process for compliance
- Identify and mitigate vulnerabilities from configuration weaknesses
- Complete coverage of the IT environment
- Focus assessment and remediation efforts more efficiently
- Increase audit efficiency
- Improve information security team's relationship with IT
- Make policy enforceable
- Keep up with the threat landscape

THE VALUE OF PRIORITIZING POLICY ENFORCEMENT

When it comes to remediation of configuration deficiencies in policy controls, one maxim should guide everything: "You can't fix everything!" Prioritization will enable the biggest positive impact on effective risk reduction. This means first responders should focus on critical systems and applications first with judicious use of exception management. The approach to prioritization will include:

- Categorize controls by business impact based on application or data classification
- Identify critical applications and systems
- Establish an initial baseline and remediation plan
- Execute the plan but be realistic – and keep the team focused on fixing first what matters most from a risk-based perspective
- Instill "continuous monitoring" into the entire policy control assessment and remediation process because this task is never done

QUALYS PC AUTOMATES CONFIGURATION SECURITY

Qualys Policy Compliance (PC) is a cloud service that performs automated security configuration assessments on IT systems throughout your network. It works in tandem with Qualys Vulnerability Management to help you to reduce risk and continuously comply with internal policies and external regulations.

Platform	Revolutionize both security & compliance with the industry's most integrated, scalable and extensible cloud platform.
Define Policies	Interactively set up IT standards for hardening configurations and complying with relevant regulations.
Specify Controls	Select host & app settings to check for each policy.
Assess	Scan and analyze OS and application configurations on each target host.
Remediate	Fix violations and configuration "drift" early – before audits – and manage exceptions centrally.
Inform	Customize comprehensive reports to document compliance for IT, business executives, risk managers and auditors.

LEARN MORE

Learn more about how Qualys PC can help your organization to automate IT security configuration compliance.

Website literature
https://www.qualys.com/enterprises/qualysguard/policy-compliance/

Free Trial
https://www.qualys.com/forms/trials/qualysguard/#/pc

SC Magazine Honors Qualys as Winner of Best Risk/Policy Management Solution Category

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, Cognizant Technology Solutions, Dell SecureWorks, Fujitsu, HCL Comnet, InfoSys, NTT, Tata Communications, Verizon and Wipro. The company is also a founding member of the Cloud Security Alliance (CSA) and Council on CyberSecurity. For more information, please visit **www.qualys.com.**

QUALYS®
CONTINUOUS 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**

© Qualys and the Qualys logo are proprietary trademarks of Qualys, Inc. All other products or names may be trademarks of their respective companies. 01/15