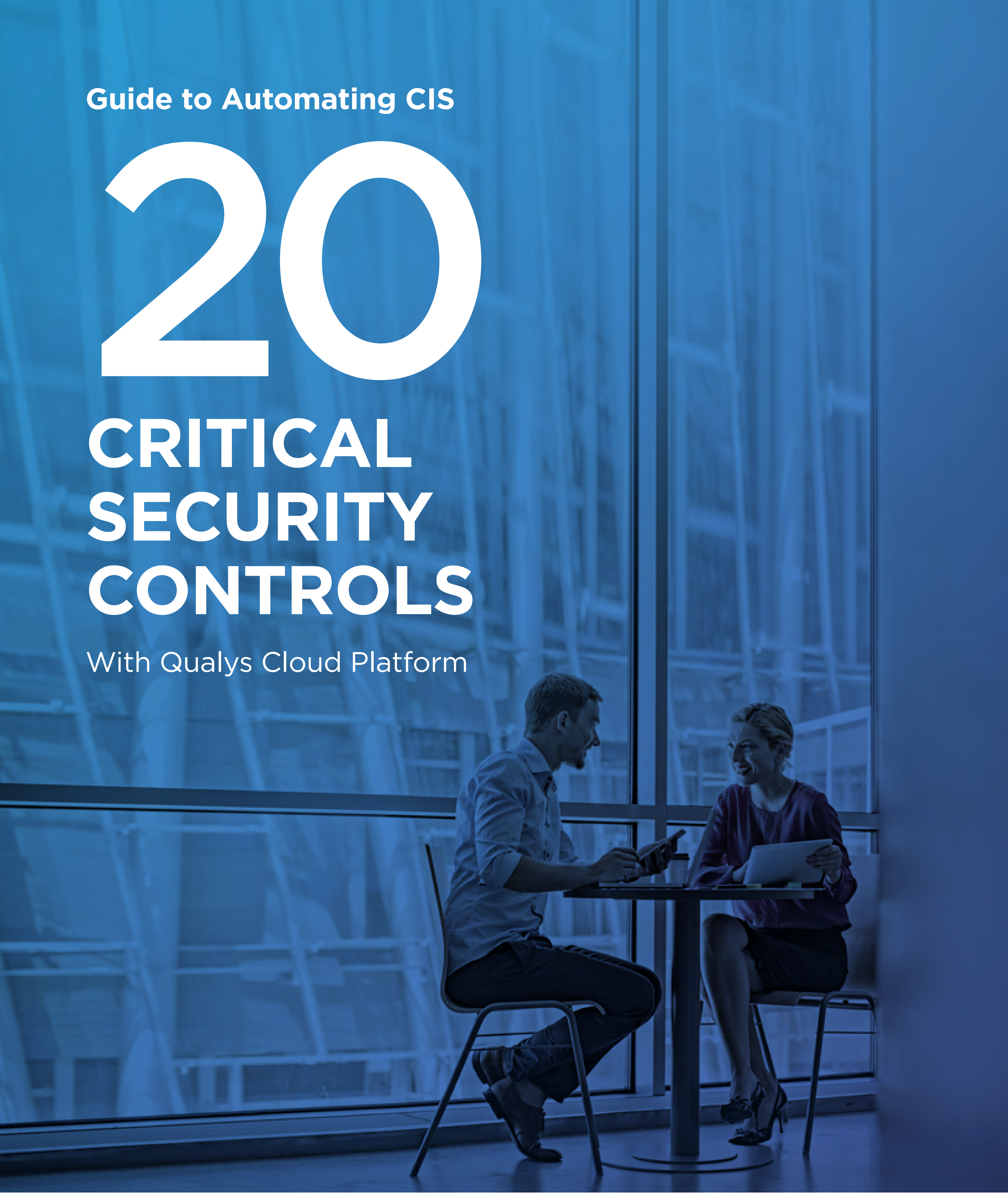
Guide to Automating CIS

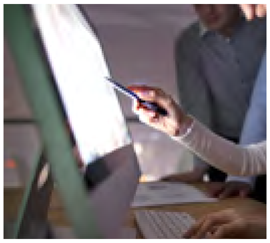
20 CRITICAL SECURITY CONTROLS

With Qualys Cloud Platform



Qualys.

Introduction



The cyber security world is a noisy place. CISOs get bombarded daily with information, including the latest research studies, threat warnings, vendor announcements, industry and regulatory mandates, best practice controls and hacking incident reports.

Keeping perspective and making sense out of it all is a challenge, especially as CISOs scramble to protect IT infrastructures whose boundaries are increasingly fluid due to the adoption of mobility, cloud computing, IoT and other new technologies.

Fortunately, there is a set of foundational InfoSec practices that offers a methodical and sensible approach for securing your IT environment: the Center for Internet Security's Critical Security Controls (CSCs).

This structured and prioritized set of best practices maps effectively to most security control frameworks, government regulations, contractual obligations and industry mandates. Developed and periodically updated by a global community of experts, the 20 controls are "the most effective and specific set of technical measures available to detect, prevent, respond, and mitigate damage from the most common to the most advanced of those attacks," according to the CIS, a non-profit organization devoted to improving cybersecurity.

How effective are these controls? According to CIS, organizations can cut their risk of cyber attack by a whopping 85 percent if they just apply the first five controls, which provide what the organization calls "foundational cyber hygiene."

In last year's SANS Institute paper "Leading Effective Cybersecurity with the Critical Security Controls", author Wes Whitteker noted that while investments in cybersecurity have boomed in recent years, so have the number and impact of major data breaches.

For Whitteker, this signals an ugly truth: The global cybersecurity problem is being met with ineffective responses, due to organizations' lack of a solid cybersecurity foundation and of a comprehensive understanding and visibility of the information infrastructure.

"If the functions that set an organization's cybersecurity foundation are flawed, it is very likely that the solutions they choose will be flawed, too," he writes. "The CSCs offer a framework that provides the critical visibility needed to aid in strategy development and manage existing organizational environments."

Ultimately, organizations that leverage the CSCs to improve their cybersecurity foundation will move unequivocally towards attaining "a resilient cybersecurity architecture … that is prepared for continuous improvement and adaptable to the latest cybersecurity threats," Whitteker writes.

SLASH RISK BY

85%

TOP 5 CIS CONTROLS

1. Inventory of authorized and unauthorized devices
2. Inventory of authorized and unauthorized software
3. Secure configurations for hardware and software on mobile devices, laptops, workstations and servers
4. Continuous vulnerability assessment and remediation
5. Controlled use of administrative privileges

The many endorsements for the controls include:

- A California Attorney General report from 2016 stated that the CSCs represent “a minimum level of information security that all organizations that collect or maintain personal information should meet” and that failing to implement them “constitutes a lack of reasonable security.”
- The U.S. National Institute of Standards and Technology (NIST) cites the CSCs as one of the “informative references” for its Framework for Improving Critical Infrastructure Cybersecurity.

As you’ll see from this whitepaper, the Qualys Cloud Platform — a single, integrated, end-to-end platform — can help security teams of any size to broadly and comprehensively adopt the CIS controls.

Its robust, scalable, and extensible architecture powers Qualys’ IT security and compliance cloud apps, giving you a continuous, always-on assessment of your global security and compliance posture, with instant visibility across all your IT assets, wherever they reside. Qualys solutions can provide in-depth assessment and validation of all critical security controls and related technologies to ensure that they are in place, properly configured, and free from vulnerabilities.

CSC #	CRITICAL SECURITY CONTROL	QUALYS APP MAPPING														
		AI	SYN	VM	PC	TP	CM	IOC	CS	WAS	WAF	CRA	FIM	SAQ	CSA	PM
CSC #1	Inventory of Authorized and Unauthorized Devices	✓	✓	✓	✓											
CSC #2	Inventory of Authorized and Unauthorized Software	✓	✓	✓	✓											
CSC #3	Secure Configurations for Hardware and Software				✓							✓			✓	
CSC #4	Continuous Vulnerability Assessment & Remediation			✓		✓	✓									✓
CSC #5	Controlled Use of Administrative Privileges				✓											
CSC #6	Maintenance, Monitoring, and Analysis of Audit Logs				✓								✓			
CSC #7	Email and Web Browser Protections			✓	✓									✓		✓
CSC #8	Malware Defenses				✓			✓		✓	✓		✓			
CSC #9	Limitation and Control of Network Ports			✓	✓		✓				✓					
CSC #10	Data Recovery Capability				✓									✓		
CSC #11	Secure Configurations for Network Devices			✓	✓											
CSC #12	Boundary Defense			✓	✓	✓	✓		✓	✓	✓					
CSC #13	Data Protection				✓								✓			
CSC #14	Controlled Access Based on the Need to Know	✓			✓				✓							
CSC #15	Wireless Access Control			✓	✓											
CSC #16	Account Monitoring and Control				✓									✓		
CSC #17	Security Skills Assessment and Appropriate Training to Fill Gaps													✓		
CSC #18	Application Software Security	✓	✓		✓			✓	✓	✓	✓					✓
CSC #19	Incident Response and Management				✓			✓					✓			✓
CSC #20	Penetration Tests and Red Team Exercises			✓		✓	✓	✓								

Now we’ll take a closer look at all of the controls, and explain how Qualys can help you implement them.

CSC 1 & CSC 2

Inventory of Authorized and Unauthorized Devices:

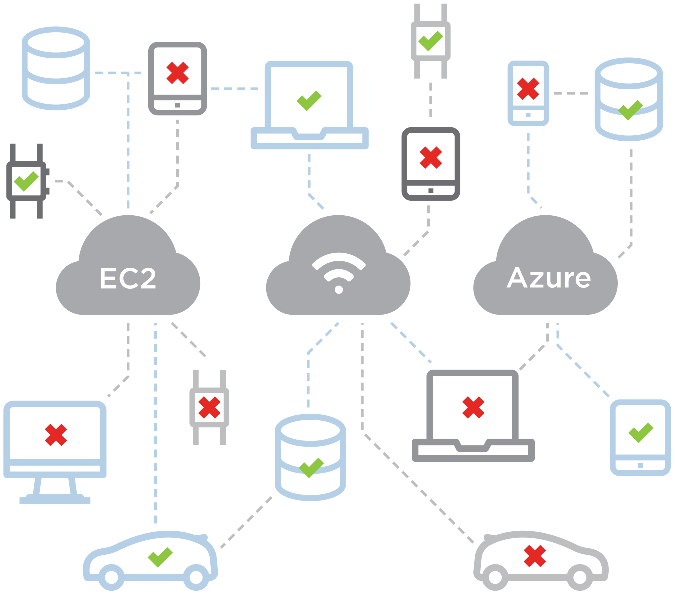
Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

Inventory of Authorized and Unauthorized Software:

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

The first two controls address the importance of having visibility into your IT environment. You can't protect — nor defend yourself from — devices and software that you don't know are in your network.

The first two controls address the importance of having visibility into your IT environment. You can't protect — nor defend yourself from — devices and software that you don't know are in your network. These blind spots are proliferating as organizations adopt technologies and processes that blur traditional network boundaries, making it easy for end users to bypass the IT department, and providing a plethora of intrusion opportunities for hackers.



These controls' recommendations include the following practices to be in place relative to the management of assets in your environment:

- ✓ Deploy an automated asset inventory discovery tool and use it to build a preliminary inventory of systems connected to an organization's public and private network(s).
- ✓ If the organization is dynamically assigning addresses using dynamic host configuration protocol (DHCP), then deploy DHCP server logging, and use this information to improve the asset inventory and help detect unknown systems.
- ✓ Devise a list of authorized software and the version that is required in the enterprise for each type of system, including servers, workstations, and laptops of various kinds and uses. This list should be monitored by file integrity checking tools to validate that the authorized software has not been modified.
- ✓ Deploy application whitelisting that allows systems to run software only if it is included on the whitelist and prevents execution of all other software on the system.

How Qualys Can Help

AI QUALYS ASSET INVENTORY (AI):

Qualys cloud-based Asset Inventory helps customers continuously discover systems — both hardware and software — connected to an organization's public and private network(s), wherever they reside. This powerful solution also maintains critical attributes of assets such as IP address, location, hardware, software information and more, providing instant visibility across your IT environment. With Qualys AI, you can achieve the first of what are known as the "first five quick wins" sub-controls, which is mentioned above: maintaining the whitelist of the software for each device.

This data is collected using a variety of tools and methods, including Qualys network scanners and Qualys' groundbreaking Cloud Agents. Qualys AI collects detailed information about assets and their components, and keeps it up to date. It provides fast searching across these attributes using a powerful search engine, and allows you to organize the systems, aligning them with their business purpose.

SYN QUALYS CMDB SYNC (SYN)

Tap powerful Qualys asset discovery and classification technology to complement the ServiceNow CMDB, providing detailed data on new and changed IT assets. The data comes from Qualys AI, which leverages Qualys' highly distributed and scalable cloud platform, and various data collection tools, including Qualys Cloud Agents, to compile and continually update a full inventory of your IT assets everywhere: on-premises, in elastic clouds and mobile endpoints.

VM PC QUALYS VULNERABILITY MANAGEMENT (VM) AND QUALYS POLICY COMPLIANCE (PC)

Qualys Vulnerability Management (VM) and Qualys Policy Compliance (PC) further augment the inventory data from the AI and SYN apps enabling you to manage and track mandatory and prohibited software, operating systems and devices. Each app has out-of-the-box signatures to check detailed requirements, such as specific software details, identification of out of date/end-of-lifed versions, service status, as
well as patch information for critical software.

Compile and continually update a full inventory of your IT assets everywhere: on-premises, in elastic clouds and mobile endpoints.

CSC 3

Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Establish, implement, and actively manage (track, report on, 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.

Critical Security Control 3 is about preventing exposure due to misconfiguration. Weak security settings, such as unchanged default passwords, ports inadvertently left open, excessive admin privileges, misconfigured certificates, faulty authentication processes, etc, are broadly exploited by cyber attackers, and — when breaches occur as a result — consequences include sharp penalties from government regulators.

Weak security settings, such as unchanged default passwords, ports inadvertently left open, excessive admin privileges, misconfigured certificates, faulty authentication processes, etc, are broadly exploited by cyber attackers

CIS recommends continuous validation of a variety of technical controls across your IT systems such as:

- ✓ Establish standard secure configurations of operating systems and software applications. Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system. These images should be validated and refreshed regularly to update their security configuration in light of recent vulnerabilities and attack vectors.
- ✓ Follow strict configuration management, building a secure image that is used to build all new systems that are deployed in the enterprise. Any existing system that becomes compromised should be re-imaged with the secure build. Regular updates or exceptions to this image should be integrated into the organization’s change management processes. Images should be created for workstations, servers, and other system types used by the organization.

How Qualys Can Help

PC QUALYS POLICY COMPLIANCE (PC)

Qualys Policy Compliance (PC) is the gold standard for assessing IT security configurations, letting you continuously reduce risk and comply with internal policies and external regulations. Qualys PC provides automated technical control assessment across a wide variety of technologies, including operating systems, network devices, server applications and databases. With out-of-the-box library content based on industry- and vendor-recommended best practices, such as the CIS Benchmarks and the Defense Information Systems Agency's (DISA) Security Technical Implementation Guides (STIGs), you can fast-track your compliance assessments, or you can customize your control requirements to suit your unique needs. Qualys PC helps you prevent configuration drift and meet a variety of regulatory requirements. It provides mandate-based reporting to easily identify areas of concern ahead of audits while optimizing the data collection process using your choice of baseline standards.

With PC, you can prioritize and track remediation and exceptions, demonstrating a repeatable, auditable process for compliance management focused on the most critical issues first.

Qualys PC enables you to completely address the second of the "first five quick wins" sub-controls, which is mentioned above and which requires organizations to establish and ensure the use of standard secure configurations for operating systems and software applications.

CSA **BETA -** QUALYS CLOUD SECURITY ASSESSMENT

Qualys Cloud Security Assessment (CSA) provides unparalleled visibility and continuous security of public cloud infrastructures so you can identify cloud assets, and assess their configurations against industry best practices from groups like CIS and vendors like Amazon AWS, Microsoft Azure, and Google Cloud. As part of Qualys' new CloudView app framework, CSA enables businesses to continuously monitor and secure their public cloud infrastructure against misconfigurations, malicious behavior, and non-standard deployments. It integrates with cloud platform providers' native APIs to continuously discover all resources and provide full visibility into your entire cloud infrastructure. It also provides topological views of the infrastructure and relationships across other cloud resources.

CRA **UPCOMING -** QUALYS CERTIFICATE ASSESSMENT

Qualys Certificate Assessment provides visibility and continuous monitoring of SSL/TLS configurations and certificates across all assets, including enabled protocols and cipher suites, along with a score to quickly highlight the security posture of the configuration. It also analyzes the algorithms and key sizes used in those certificates, quickly allowing isolation and remediation of certificates with weaker keys or algorithms.

CSC 4

Continuous Vulnerability Assessment and Remediation

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

Thousands of new software vulnerabilities are disclosed every year, each one representing a potential opportunity for hackers to break into a network. That's why organizations must know at all times which vulnerabilities are present in their IT assets; understand the level of risk each one carries; and plan and prioritize remediation of affected IT assets accordingly. Critical Security Control 4 directs organizations to properly manage vulnerabilities so that they can "immunize" their IT assets against the most common cyber attacks: opportunistic strikes designed to exploit common, disclosed vulnerabilities.

Organizations must know at all times:

- Which vulnerabilities are present in their IT assets
- The level of risk each one carries
- Remediation of affected IT assets

CIS recommendations include:

✓ Run automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis and deliver prioritized lists of the most critical vulnerabilities to each responsible system administrator, along with risk scores that compare the effectiveness of system administrators and departments in reducing risk. Use a SCAP-validated vulnerability scanner that looks for both code-based vulnerabilities (such as those described by Common Vulnerabiliies and Exposures (CVE) entries) and configuration-based vulnerabilities (as enumerated by the Common Configuration Enumeration Project).

✓ Correlate event logs with information from vulnerability scans to fulfill two goals.

- First, personnel itself should verify that the activity of the regular vulnerability scanning tools itself is logged.
- Second, personnel should be able to correlate attack detection events with prior vulnerability scanning results to determine whether the given exploit was used against a target known to be vulnerable.

How Qualys Can Help

VM QUALYS VULNERABILITY MANAGEMENT (VM)

Qualys Vulnerability Management (VM) gives you immediate, global visibility into where your IT systems might be vulnerable to the latest threats, and how to protect them. It helps you to continuously secure your IT infrastructure, so that your organization can withstand attacks seeking to exploit unpatched and improperly configured systems.

Qualys VM assigns remediation tickets, manages exceptions, lists required patches for each host, integrates with existing IT ticketing systems, and generates comprehensive reports to help drive remediation of found vulnerabilities.

CM QUALYS CONTINUOUS MONITORING (CM)

Qualys Continuous Monitoring (CM) enables customers to receive immediate notifications of newly identified issues in order to proactively address potential problems, providing continuous surveillance of both internal and external hosts, enabling infrastructure teams to reduce exposure.

TP QUALYS THREAT PROTECTION (TP)

Qualys Threat Protection (TP) helps you automatically prioritize the vulnerabilities that pose the greatest risk to your organization by correlating active threats against your vulnerabilities. Qualys TP includes a Live Threat Intelligence Feed where Qualys security engineers continuously validate and rate new threats from internal and external sources, highlighting emerging concerns about vulnerabilities that pose an immediate threat to your business, including details about which assets may be affected.

Qualys TP allows teams to quickly visualize which of our systems are exposed to active threats, such as zero-days, denial-of-service attacks, actively attacked vulnerabilities, and easy exploits requiring little scills or vulnerabilities lacking a patch. Qualys TP provides you with the ability to measure your progress and remediation efforts with real-time trend analysis and receive notifications when critical exposures emerge.

PM **UPCOMING -** QUALYS PATCH MANAGEMENT (PM)

Qualys Patch Management (PM) will enable remediation at scale by deploying security patches to operating systems and applications to remediate code-based vulnerabilities.

With the combination of Qualys VM, CM, and TP, you'll also address the third of the "first five quick wins" sub-controls, which is mentioned above and which requires customers to run automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis.

In addition, with Qualys VM and PM, you'll address the fourth of these "quick wins" sub-controls: Deployment of automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe.

CSC 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.

Users with administrative privileges are particularly attractive for hackers. Compromising one of those accounts gives intruders broad access within the breached device and network, boosting their ability to do harm. Consequently, InfoSec teams must closely monitor these accounts. Critical Security Control 5 requires minimizing the use of administrative privileges.

CIS recommendations include:

- ✓ Minimizing administrative privileges, only using these accounts when required, auditing the use of administrative privileged functions, and monitoring anomalous behavior.
- ✓ Using automated tools to inventory administrative accounts and validating that users with admin privileges on desktops, laptops, and servers are authorized by a senior executive.
- ✓ Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration-level accounts.

How Qualys Can Help

PC QUALYS POLICY COMPLIANCE (PC)

Qualys Policy Compliance (PC) account controls provide full visibility into accounts with administrative privileges, so you can validate that they're being used only where needed. This helps you address the last of the "first five quick wins" sub-controls, which is mentioned above and which discusses the need to minimize administrative privileges and only use administrative accounts when required.

Qualys PC hosts a variety of related out-of-the-box controls to check processes, files and objects for valid permissions. Group membership and rights for Windows systems as well as "User Account controls (UAC)" can also be validated in order to help organizations minimize the use of the administrative accounts/access.

Users with administrative privileges are particularly attractive for hackers.

CSC 6

Maintenance, Monitoring, and Analysis of Audit Logs

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

Another critical security element are audit logs, because often they provide the only clear evidence of insider or stealthy attacks. For this reason, InfoSec teams must make sure to activate the logging capabilities that come with most operating systems, network services, and firewall technologies. Logs should be comprehensive, accurate, and centrally stored so that they can be mined for insights, audits, and, when needed, incident response. Critical Security Control 6 defines requirements for managing audit logs to meet these needs.

CIS recommendations include:

- ✓ Include at least two synchronized time sources from which all servers and network equipment retrieve time information on a regular basis so that timestamps in logs are consistent.
- ✓ Validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and other elements of each packet and/or transaction. Make sure systems record logs in a standardized format, and if this is impossible, deploy log normalization tools.
- ✓ Ensure that all systems that store logs have adequate storage space. Archive and digitally sign logs periodically.

How Qualys Can Help

PC QUALYS POLICY COMPLIANCE (PC)

Qualys Policy Compliance (PC) helps organizations validate key aspects of audit log configuration on a breadth of technologies including operating systems, network devices (including firewalls), database servers, and other server software. This includes validating related critical settings, such as synchronized time sources, configuration of file auditing settings, and logging storage and permissions.

FIM QUALYS FILE INTEGRITY MONITORING (FIM)

Qualys File Integrity Monitoring (FIM) tracks file changes across global IT systems, including changes to security settings for log files, helping you detect and identify potential tampering with log files and critical settings. File Audit attributes changes can also be tracked, to make sure that critical logging of access to files is being logged by the underlying operating system. Qualys FIM comes with out-of-the-box monitoring profiles based on industry best practices and vendor-recommended guidelines to make sure you are monitoring the correct sensitive operating system and application files. FIM logs file modification events centrally as well, providing another avenue of security event analysis to protect against more complex attacks while also providing a means to enforce change-control policies in your IT environment.

CSC 7

Email and 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.

Hackers do their best to turn web browsers and email clients into traps to trick end users into performing actions that will help them gain access to their IT environment. For example, via phishing and social engineering methods, hackers try to fool email recipients into opening malware-laden attachments and clicking on legitimate-looking links that take users to malicious sites, and inadvertently providing sensitive, confidential data in the process.

Cyber criminals also attempt to compromise web browsers in multiple ways, such as by using automated self-updating exploit kits to compromise endpoints to get behind your network perimeter.

Thus, it's crucial for InfoSec teams to secure these two attractive breach vectors.

CIS recommendations include:

- ✓ Using only fully supported web browsers and email clients, and, ideally, only the latest version of the browsers, because they have the vendors' latest security functions and fixes.
- ✓ Uninstalling or disabling unnecessary or unauthorized browser or email client plugins or add-ons. Each plugin shall utilize application / URL whitelisting and only allow the use of the application for pre-approved domains.
- ✓ Limiting unnecessary scripting languages in web browsers and email clients, including ActiveX and JavaScript on systems that don't need such capabilities.

How Qualys Can Help

VM QUALYS VULNERABILITY MANAGEMENT (VM)

Qualys Vulnerability Management (VM) assesses the vulnerabilities of software on the endpoint with special attention on web browsers and email clients. It will identify out-of-date versions that may no longer be secure and ensure that no required critical patches are missing. It also validates critical ActiveX, Java, Adobe and other plug-in versions to make sure that vulnerabilities are known so they can be patched promptly.

PC QUALYS POLICY COMPLIANCE (PC)

Qualys Policy Compliance (PC) can assess the configurations of the web browsers against CIS benchmark recommendations, to make sure that high-risk settings are disabled that may automatically execute plug-ins, scripts, and other content that can increase risk of compromise.

SAQ QUALYS SECURITY ASSESSMENT QUESTIONNAIRE (SAQ)

Qualys Security Assessment Questionnaire (SAQ) provides out-of-the-box questionnaires which can be distributed to internal and external parties to assess the effectiveness of your training and awareness programs, created to protect against phishing and social engineering methods.

PM **UPCOMING -** QUALYS PATCH MANAGEMENT (PM)

Qualys Patch Management will ensure that browsers are updated by deploying their most recent version, mitigating the risk that infiltration could occur via human interaction with malicious payloads.

CSC 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 corrective action.

Malware is a key component of cyber attacks and continues to be an arms-race between InfoSec professionals and hackers. Malware can be used to compromise a wide variety of IT assets and can be deployed via many different avenues, including email attachments, malicious web pages, cloud services and removable media (such as USB devices). Keeping up with the constant change in malware delivery and obfuscation techniques is a significant challenge requiring that a variety of controls be in place as defined in Critical Security Control 8.

CIS recommendations include:

- ✓ Employ automated tools to continuously monitor workstations, servers, and mobile devices with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality. All malware detection events should be sent to enterprise anti-malware administration tools and event log servers.

- ✓ Employ anti-malware software that offers a centralized infrastructure that compiles information on file reputations or have administrators manually push updates to all machines. After applying an update, automated systems should verify that each system has received its signature update.

- ✓ Limit use of external devices to those with an approved, documented business need. Monitor for use and attempted use of external devices. Configure laptops, workstations, and servers so that they will not auto-run content from removable media, like USB tokens (i.e., “thumb drives”), USB hard drives, CDs/DVDs, FireWire devices, external serial advanced technology attachment devices, and mounted network shares. Configure systems so that they automatically conduct an antimalware scan of removable media when inserted.

How Qualys Can Help

QUALYS WEB APPLICATION SCANNING (WAS) AND WEB APPLICATION FIREWALL (WAF)

Qualys Web Application Scanning (WAS) and Web Application Firewall (WAF) are natively and tightly integrated for seamless identification and mitigation of risks and offer a complete solution for web app security.

Qualys WAS is a robust DAST (Dynamic Application Security Testing) product that identifies security holes in web applications, SOAP web services, and RESTful APIs, through continuous discovery of HTTP services and detection of vulnerabilities and misconfigurations. Qualys WAS easily scales to scan thousands of web applications while covering the OWASP Top 10 vulnerabilities and more. Its malware detection functionality scans an organization's internet-facing websites, and identifies and reports infections, including zero-day threats via behavioral analysis. Detailed malware infection reports are provided for remediation. A central dashboard displays scan activity, infected pages and malware infection trends, and lets users initiate actions directly from its interface.

Meanwhile, Qualys WAF blocks attacks and lets you virtually patch web app vulnerabilities. It can be quickly deployed for apps on public or private clouds, and scaled quickly. Application traffic stays in your environment to minimize latency and maintain control.

QUALYS INDICATION OF COMPROMISE (IOC)

Qualys Indication of Compromise (IOC) continuously monitors endpoints to detect suspicious activity, flagging telemetry data that could indicate malware or breaches on devices on and off the network. Qualys IOC uses the Qualys Cloud Agent's non-intrusive data collection and delta processing techniques to continuously and transparently capture endpoint activity information in a way that is better than other solutions' query-based approaches or distributed data collectors.

Analysis, hunting, and threat indicator processing is performed in the cloud on billions of active and past endpoint events. Those results are then coupled with threat intelligence data from Qualys Malware Labs and third-party threat intelligence sources to identify malware infections (indicators of compromise) and threat actor actions (indicators of activity).

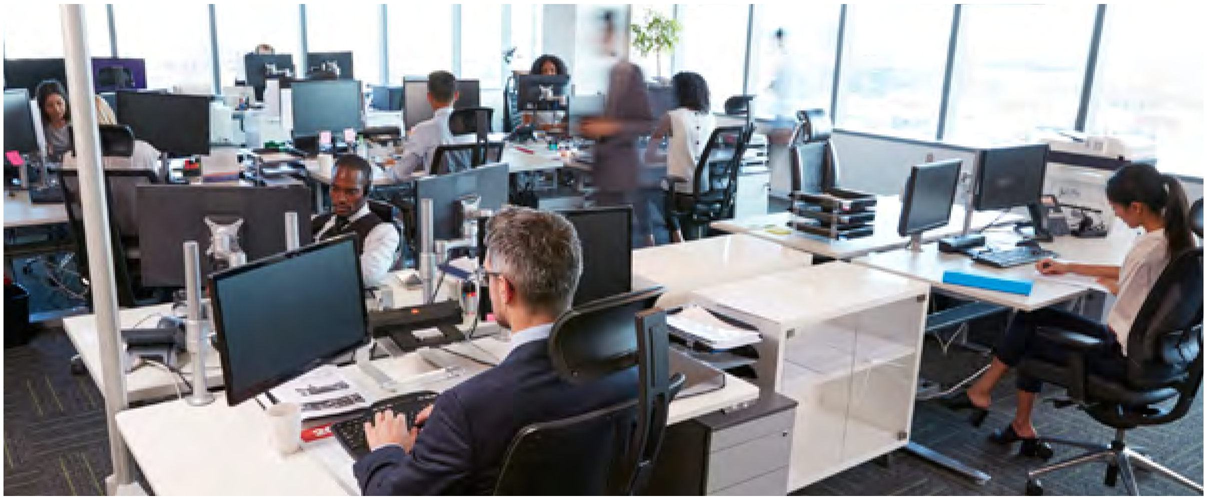
QUALYS POLICY COMPLIANCE (PC)

Qualys Policy Compliance (PC) allows customers to validate the configuration settings of anti-virus solutions, as well as check the list of running processes and software for potential malicious entries.

QUALYS FILE INTEGRITY MONITORING (FIM)

Qualys File Integrity Monitoring (FIM) can serve as a last line of detection, identifying changes to critical operating system and configuration files that may indicate a targeted attack or specially designed root-kit has been put in place.

CSC 9



Limitation and 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.

Hackers constantly look for remotely accessible network services vulnerable to exploitation, such as poorly configured web, mail, file, and print servers, and domain name system (DNS) servers installed by default on a variety of devices, often without a business need. Many software packages automatically install and activate services without alerting users or administrators. Critical Security Control 9 calls for limiting unnecessary services to reduce potential exposures to attack.

CIS recommendations include:

- ✓ Ensure that only ports, protocols, and services with validated business needs are running on each system.
- ✓ Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.
- ✓ Perform automated port scans on a regular basis against all key servers and compare to a known effective baseline. If a change that is not listed on the organization’s approved baseline is discovered, an alert should be generated and reviewed.
- ✓ Verify any server that is visible from the internet or an untrusted network, and if it is not required for business purposes, move it to an internal VLAN and give it a private address.

A Deep Tech Dive Into WAF & CSC9

Custom rules allow restricting the access to the application using perimetric criterias, such as source-IP address/range, autonomous system, geo-location, or plenty of others, such as user agent, custom header, transaction latency, or parameter name or value. Configuration changes are done on the Qualys Cloud Portal and tracked by WAF appliances through outgoing, self-initiated TCP-443 http/s transactions to the cloud, with support of outgoing proxy mode. That way, the appliance is fully dedicated to processing the traffic while guaranteeing the configuration's integrity. Appliances require outbound DNS, NTP and, optionally, SYSLOG services to be fully operational (UDP:53,123,514; TCP:514).

How Qualys Can Help

VM QUALYS VULNERABILITY MANAGEMENT (VM)

Qualys Vulnerability Management (VM) scans the organization's assets for open ports and services, and processes, allowing you to quickly identify services so they can be analyzed for importance.

CM CONTINUOUS MONITORING (CM)

Continuous Monitoring (CM), an add-on to VM, enables you to receive immediate notification when new issues are identified on internal and external hosts, such as a new port, service, or other identified software, allowing teams to rapidly address potential problems. Once a baseline is established you can easily maintain that baseline to prevent configuration drift and accidental exposure as well as quickly identify potential compromise.

PC QUALYS POLICY COMPLIANCE (PC)

Qualys Policy Compliance (PC) assesses the organization's hosts from the inside-out, to make sure that only required services and applications are running and that initial baseline configurations remain constant. Unnecessary ports and services that should be blocked or disabled are quickly identified. Recommended services are a key component of many of the out-of-the-box library policies provided with PC.

WAF QUALYS WEB APPLICATION FIREWALL (WAF)

Qualys Web Application Firewall (WAF) is an inline virtual appliance that terminates both client-side and server-side traffic on a single NIC. In addition to Secure Shell (SSH) for admin purposes, it opens http/s sockets on requested TCP ports (TCP 80, 443 or any transposed port).

CSC 10

Data Recovery Capability

The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

After compromising machines, attackers often make significant changes to configurations and software, and subtle alterations to data, potentially jeopardizing organizational effectiveness with polluted information. After the attack is detected, it can be extremely difficult for organizations without a trustworthy data recovery capability to remove all aspects of the attacker's presence on the machine. Critical Security Control 10 requires good backup and recovery practices to be in place to speed incident recovery.

CIS recommendations include:

- ✓ Ensure each system is automatically backed up at least weekly, and more often for systems storing sensitive information. To rapidly restore a system from backup, the operating system, application software, and data should each be included in the overall backup procedure. All backup policies should be.
- ✓ Test data on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.

How Qualys Can Help

PC QUALYS POLICY COMPLIANCE (PC)

Qualys Policy Compliance (PC) assesses key configuration settings related to backups and restore features for a variety of technologies, such as databases and server applications. For example, if backup for a SQL database is enabled, then replication is enabled. The presence of mandatory software, such as backup software, can also be confirmed.

SAQ QUALYS SECURITY ASSESSMENT QUESTIONNAIRE (SAQ)

Qualys Security Assessment Questionnaire (SAQ) provides out-of-the-box questionnaires that can be used to assess backup and restore processes and procedures. Critical details of the disaster recovery process can be collected and validated against internal policies and best practices. You can make assessments based on the responses of internal and external parties, and validate that the entire process has been tested and reviewed.

Ensure each system is automatically backed up at least weekly, and more often for systems storing sensitive information.

CSC 11

Secure Configurations for Network Devices

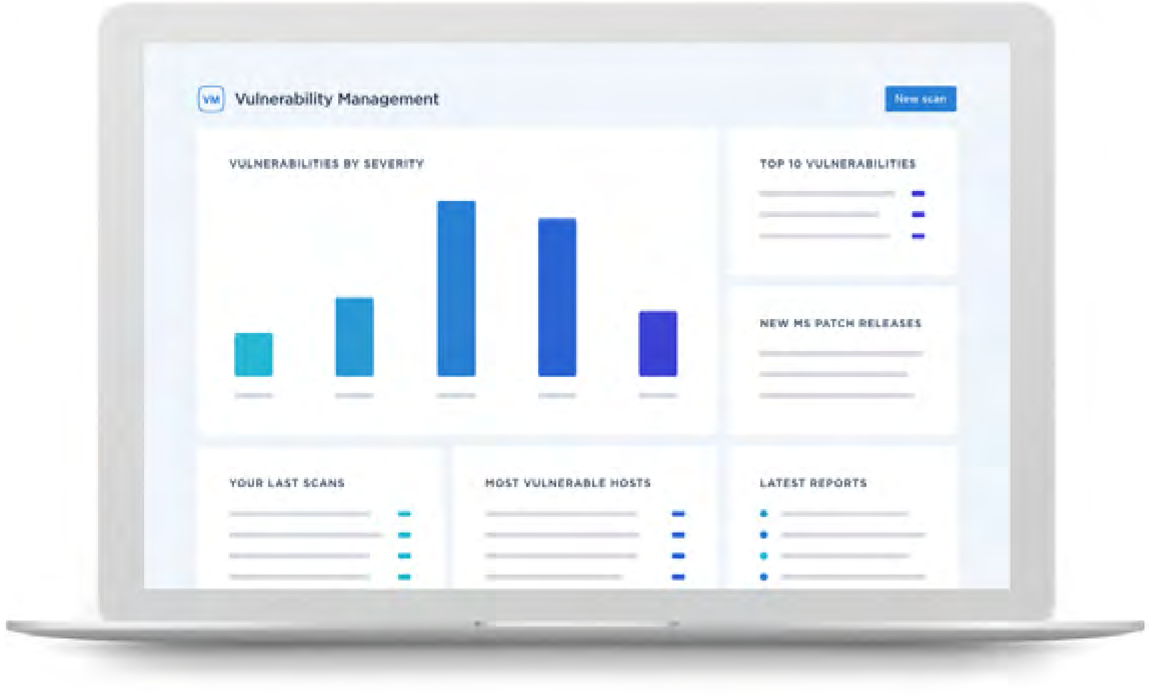
Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

When attackers exploit flaws in these devices, they gain access to networks, redirect traffic on a network, and intercept information.

The default configurations with which vendors ship network infrastructure devices are aimed at simple deployments and ease of use, not security: open services and ports, default accounts or passwords, support for older (vulnerable) protocols, pre-installation of unneeded software. Once deployed, these devices often become less secure as users request configuration exceptions. When attackers exploit flaws in these devices, they gain access to networks, redirect traffic on a network, and intercept information. Critical Security Control 11 establishes guidelines for securing these devices.

CIS recommendations include:

- ✓ Compare firewall, router, and switch configuration against standard secure configurations defined for each type of network device in use in the organization. The devices' security configuration should be documented, reviewed, and approved by an organization change control board. Any deviations from the standard configuration, or updates to the standard configuration, should be documented and approved in a change control system.
- ✓ All new configuration rules beyond a baseline-hardened configuration that allow traffic to flow through network security devices, such as firewalls and network-based IPs, should be documented and recorded in a configuration management system, with a specific business reason for each change, a specific individual's name responsible for that business need, and an expected duration of the need.
- ✓ Use automated tools to verify standard device configurations and detect changes. All alterations to such files should be logged and automatically reported to security personnel.



How Qualys Can Help

VM QUALYS VULNERABILITY MANAGEMENT (VM)

Qualys Vulnerability Management (VM) continuously discovers and maps each device on the organization's network, including applications on the perimeter, internal networks, and cloud provider networks, and assesses them for security vulnerabilities. Vulnerabilities can easily be identified and tracked to drive remediation efforts.

PC QUALYS POLICY COMPLIANCE (PC)

Qualys Policy Compliance (PC) lets you continuously reduce risk and comply with internal policies and external regulations. As with CSC 5, which requires similar configuration and control review for operating systems and software, Qualys PC provides automated technical control assessment across many network devices from vendors including Cisco, Juniper, and Palo Alto. Customizable out-of-the-box library content based on industry- and vendor-recommended best practices such as CIS Benchmarks and DISA STIG are also provided to fast-track your compliance assessments, or you can establish gold-standard configurations and identify drift from the original hardened configuration settings.

CSC 12

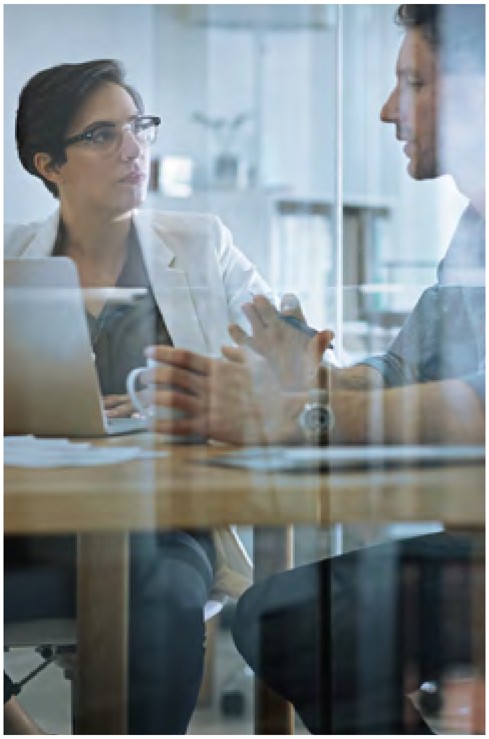
Boundary Defense

Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.

Attackers focus on systems that they can reach across the internet, exploit configuration and architectural weaknesses to gain initial access into an organization and then get deeper inside the boundary to steal information or to set up a persistent presence for later attacks. InfoSec teams must control traffic flow through network borders and police content by looking for attacks and evidence of compromised machines.

CIS recommendations include:

- ✓ Deny communications with (or limit data flow to) known malicious IP addresses (blacklists), or limit access only to trusted sites (whitelists). Tests can be periodically carried out by sending packets from bogon source IP addresses (non-routable or otherwise unused IP addresses) into the network to verify that they are not transmitted through network perimeters. Lists of bogon addresses are publicly available on the internet from various sources.
- ✓ On DMZ networks, configure monitoring systems (which may be built into IDS sensors or deployed as a separate technology) to record at least packet header information, and preferably full packet header and payloads of the traffic destined for or passing through the network border. This traffic should be sent to a properly configured Security Information Event Management (SIEM) or log analytics system so that events can be correlated from all devices on the network.



How Qualys Can Help

VM QUALYS VULNERABILITY MANAGEMENT (VM)

Qualys Vulnerability Management (VM) can scan remote devices from different network vantage points, including externally, to identify potential openings that put data at risk.

CM QUALYS CONTINUOUS MONITORING (CM)

Coupled with Qualys Continuous Monitoring (CM), recurrent scans can be completed to keep you constantly up to date about new services and ports on internal devices, as well as external devices exposed to the internet.

TP QUALYS THREAT PROTECTION (TP)

Adding Qualys Threat Protection (TP) provides threat intelligence about the latest vulnerability disclosures and maps them to your impacted IT assets whether internal or exposed to the internet. The three apps combined provide the comprehensive coverage needed to protect your perimeter.

PC QUALYS POLICY COMPLIANCE (PC)

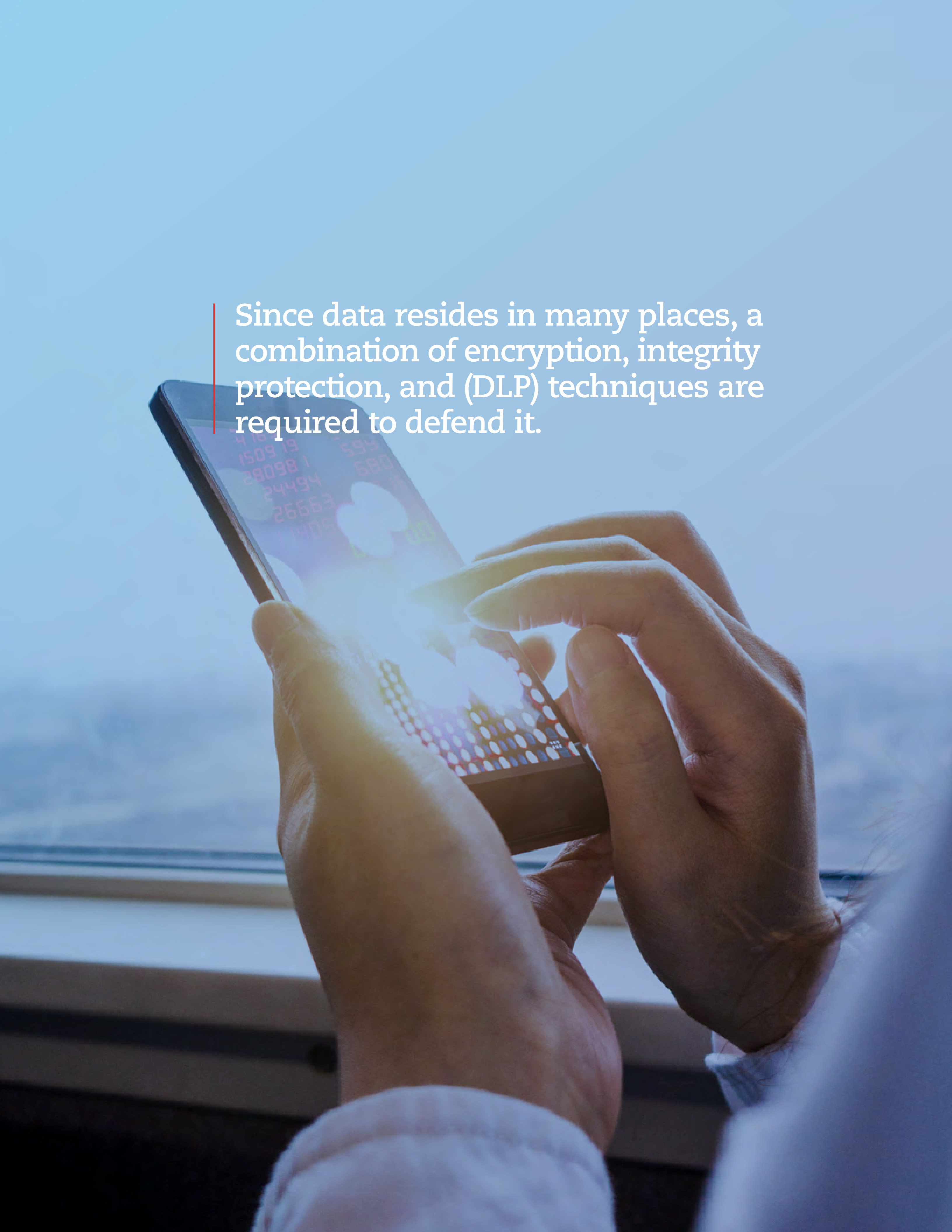
Qualys Policy Compliance (PC) can be used to assess configuration of network devices and firewalls to ensure the boundary is properly protected and help prevent configuration drift for key security settings on such devices. A wide array of out-of-the-box content is available to ensure proper configuration of the perimeter network, which can be customized to fit an organization's unique needs.

WAS WAF QUALYS WEB APPLICATION SCANNING (WAS) AND WEB APPLICATION FIREWALL (WAF)

Qualys offers a complete solution for web app security with Qualys Web Application Scanning (WAS) and Web Application Firewall (WAF), which are natively and tightly integrated, giving you a single, interactive console for web app vulnerability detection (WAS) and attack protection (WAF) for seamless identification and mitigation of risks. Qualys WAS is a robust DAST (Dynamic Application Security Testing) product that identifies security holes in web applications, SOAP web services, and RESTful APIs, through continuous web app discovery of HTTP services and detection of vulnerabilities and misconfigurations. Identified vulnerabilities from WAS can be virtually patched in WAF with the push of a button, thereby protecting you from exploitation even in the case where the application developers are unable to remediate the code.

CS QUALYS CONTAINER SECURITY (CS)

Qualys CS lets organizations discover, track, and continuously protect containers in DevOps pipelines and deployments across cloud and on-premises environments. This helps ensure that the boundary settings of the containers are assessed on a continuous basis.



Since data resides in many places, a combination of encryption, integrity protection, and (DLP) techniques are required to defend it.

CSC 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.

Since data resides in many places, a combination of encryption, integrity protection, and (DLP) techniques are required to defend it.

Care should also be taken to ensure that products used within an enterprise implement well known and vetted cryptographic algorithms, as identified by NIST. Re-evaluation of the algorithms and key sizes used within the enterprise on an annual basis is also recommended to ensure that organizations are not falling behind in the strength of protection applied to their data.

CIS recommendations include:

- ✓ Perform an assessment of data to identify sensitive information that requires the application of encryption and integrity controls.
- ✓ Deploy approved hard drive encryption software to mobile devices and systems that hold sensitive data.
- ✓ Deploy an automated tool on network perimeters that monitors for sensitive information (e.g., personally identifiable information), keywords, and other document characteristics to discover unauthorized attempts to exfiltrate data across network boundaries and block such transfers while alerting information security personnel.

How Qualys Can Help

PC QUALYS POLICY COMPLIANCE (PC)

Qualys Policy Compliance (PC) has a number of out-of-the-box controls for checking the security and permissions on sensitive, critical files and processes, while making sure file transfer options are either restricted or blocked. Qualys PC can also validate that required software such as DLP solutions are in place on critical assets.

FIM QUALYS FILE INTEGRITY MONITORING (FIM)

Qualys File Integrity Monitoring (FIM) monitors and tracks changes to critical files, including changes to important security settings and file attributes to help you detect and track critical changes and incidents, while monitoring the integrity of the sensitive data.

CSC 14

Controlled Access Based on the Need to Know

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

Organizations should carefully identify and separate their most sensitive and critical assets from less sensitive, publicly accessible information on their internal networks. In many environments, internal users have access to all or most of the critical assets. Sensitive assets may also include systems that provide management and control of physical systems. Once attackers have penetrated such a network, they can easily find and exfiltrate important information, cause physical damage, or disrupt operations.

Organizations should carefully

IDENTIFY & SEPARATE

their most sensitive and critical assets from less sensitive, publicly accessible information on their internal networks.

CIS recommendations include:

- ✓ Segment the network based on the label or classification level of the information stored on the servers. Locate all sensitive information on separate VLANS with firewall filtering to ensure that only authorized individuals are only able to communicate with systems necessary to fulfill their specific responsibilities.
- ✓ All communication of sensitive information over less trusted networks should be encrypted. Whenever information flows over a network with a lower trust level, the information should be encrypted.
- ✓ All network switches will enable Private Virtual Local Area Networks (VLANs) for segmented workstation networks to limit the ability of devices on a network to directly communicate with other devices on the subnet and limit an attacker's ability to laterally move to compromise neighboring systems.

How Qualys Can Help

AI QUALYS ASSET INVENTORY (AI)

Qualys Asset Inventory (AI) can help identify and track critical systems to ensure they are organized and tracked according to their business purpose. The wealth of inventory data can help ensure that only necessary software is installed for the business purpose to help maintain proper segmentation.

PC QUALYS POLICY COMPLIANCE (PC)

Qualys Policy Compliance (PC) has a number of out-of-the-box controls for checking the security and permissions on sensitive, critical assets (e.g., information, resources and systems in the traditional data centers as well as in the cloud infrastructure) and for making sure access is only provided on a need-to-know basis. Network security controls addressed in other CSCs can also be applied here to validate proper network segmentation and the security of critical network devices.

CS QUALYS CONTAINER SECURITY (CS)

Qualys Container Security (CS) lets organizations discover, track, and continuously protect containers in DevOps pipelines and deployments across cloud and on-premises environments, ensuring that the data access outside the boundary of the containers is restricted.

CSC 15

Wireless Access Control

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

Unsecured access points give attackers convenient entry points into your IT environment, bypassing security perimeters. Attack methods include compromising employees' wireless devices and using them to enter your network, as well as planting rogue wireless access points in your organization, providing unrestricted access for intruders.

CIS recommendations include:

- ✓ Ensure that wireless devices connected to the network match an authorized configuration and security profile, with a documented owner of the connection and a defined business need. Deny access to wireless devices lacking such a configuration and profile.
- ✓ Configure network vulnerability scanning tools to detect wireless access points connected to the wired network. Reconcile identified devices against a list of authorized wireless access points. Deactivate unauthorized access points.
- ✓ Use wireless intrusion detection systems (WIDS) to identify rogue wireless devices and detect attack attempts and successful compromises. All wireless traffic should be monitored by WIDS as traffic passes into the wired network.

How Qualys Can Help

VM PC QUALYS VULNERABILITY MANAGEMENT (VM)
AND POLICY COMPLIANCE (PC)

Qualys Vulnerability Management (VM) and Policy Compliance (PC) have out-of-the-box content to assess and report on the vulnerabilities and configuration settings of wireless controllers and wireless settings on the systems, to make sure unauthorized connections are disabled, and access is provided in a secure manner.

CSC 16

Account Monitoring and Control

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

Managing accounts is a critical aspect of protecting organizations' data. Inadequate password rotation, accounts that have gained privileges as users change roles, and validation of account and privilege revocation are all critical user-account management tasks. For example, inactive but undeleted user accounts — belonging to former employees or temporary contractors — can be used by both external hackers and rogue insiders to disguise themselves as legitimate users and carry out their attacks.

CIS recommendations include:

- ✓ Review all system accounts and disable any account that cannot be associated with a business process and owner.
- ✓ Ensure that all accounts have an expiration date that is monitored and enforced.
- ✓ Establish and follow a process for revoking system access by disabling accounts immediately upon termination of an employee or contractor. Disabling instead of deleting accounts allows preservation of audit trails.
- ✓ Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.

How Qualys Can Help

PC QUALYS POLICY COMPLIANCE (PC)

Qualys Policy Compliance (PC) provides out-of-the-box content to validate the lifecycle of system/user accounts, their credentials, and privileges. PC can help organizations implement strong account controls by validating that the OS's capabilities for account management, credential requirements, privileges, and other settings are in line with their password policy, auditor requirements, and industry best practices.

SAQ QUALYS SECURITY ASSESSMENT QUESTIONNAIRE (SAQ)

Qualys Security Assessment Questionnaire (SAQ) supports out-of-the-box a shared assessment questionnaire template to assess the responses from internal and external parties regarding vendor access and monitoring, best practices for account management workflows, and monitoring that the organization's resources are in place.

CSC 17

Security Skills Assessment and 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.

CSC 17 addresses the very important element of human behavior and its impact on security. Ensuring that individuals know what is expected of them as they participate in system design, implementation, operation, use, and oversight is critical to good information security practices. Developers, IT ops pros, security analysts, end users, and executives should all be aware of security best practices, corporate policy, and incident reporting processes. If they haven’t been properly educated and trained, they could inadvertently endanger the security of your IT environment in a variety of serious ways.

CIS recommendations include:

- ✓ Perform gap analysis to see which skills employees need to implement the other Controls, and which behaviors employees are not adhering to, using this information to build a baseline training and awareness roadmap for all employees.

- ✓ Deliver training to fill the skills gap. If possible, use more senior staff to deliver the training. Or have outside teachers provide training on-site so the examples used will be directly relevant. If you have small numbers of people to train, use training conferences or online training to fill the gaps.

- ✓ Implement a security awareness program that:
  - focuses on the methods commonly used in intrusions that can be blocked through individual action
  - is delivered in short online modules convenient for employees
  - is updated frequently (at least annually) to represent the latest attack techniques
  - is mandated for completion by all employees at least annually
  - is reliably monitored for employee completion
  - and includes the senior leadership team's personal messaging, involvement in training, and accountability through performance metrics

How Qualys Can Help

SAQ QUALYS SECURITY ASSESSMENT QUESTIONNAIRE (SAQ)

Qualys Security Assessment Questionnaire (SAQ) supports a shared assessment template to assess the knowledge levels of internal and external parties on security training and awareness programs by consolidating their responses, allowing the organization to report on the programs.

CSC 18

Application Software Security

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

Attacks often exploit vulnerabilities found in web-based and other application software. Vulnerabilities can be present for many reasons, including coding mistakes, logic errors, incomplete requirements, and failure to test for unusual or unexpected conditions. Attackers are attuned to the constant stream of vulnerability disclosures, because, when left unpatched, they each represent an opportunity to breach a system by injecting specific exploits.

CIS recommendations include:

- ✓ For all commercial application software, check that the version you are using is still supported by the vendor. If not, update to the most current version and install all relevant patches and vendor security recommendations.
- ✓ Protect web applications by deploying web application firewalls (WAFs) that inspect all traffic for common attacks, including cross-site scripting, SQL injection, command injection, and directory traversal attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type.
- ✓ For in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.

How Qualys Can Help

VM QUALYS VULNERABILITY MANAGEMENT (VM)

Qualys Vulnerability Management (VM) can identify known vulnerabilities in application software such as databases, web servers, and middleware in the same way that it does for OS vulnerabilities. Multiple signatures exist to identify weak encryption configuration for legacy protocols, along with signatures to identify applications no longer supported by the vendor (EOL).

AI QUALYS ASSET INVENTORY (AI)

Qualys Asset Inventory (AI) provides complete visibility and the ability to group software installations across the entire IT environment, so that organizations can plan and prioritize their efforts to secure applications.

PC QUALYS POLICY COMPLIANCE (PC)

Qualys Policy Compliance (PC) provides controls to assess default configurations and security settings as per the best practices to prevent from the exploitable exposures. It provides recommended configurations including default credentials setup for many widely used applications.

IOC QUALYS INDICATION OF COMPROMISE (IOC)

Qualys Indication of Compromise (IOC) provides the ability to continuously monitor applications and their hosting OS in order to detect suspicious activity, flagging telemetry data that could indicate malicious activity in the application.

CS QUALYS CONTAINER SECURITY (CS)

Qualys Container Security (CS) lets organizations discover, track, and protect containers in DevOps pipelines and deployments across cloud and on-premises environments, through continuous vulnerability assessments of Docker images and underlying hosts.

WAS QUALYS WEB APPLICATION SCANNING (WAS)

Qualys Web Application Scanning (WAS) can insert security into application development and deployment in DevSecOps environments. With WAS and its API capability, you can automate scans as part of the build process to detect security flaws early and often, and automatically deliver detailed reports for review and remediation. With its flexible scheduling features and tight integration with Qualys WAF, WAS can continuously monitor and virtually patch vulnerabilities in production web apps.

PM **UPCOMING -** QUALYS PATCH MANAGEMENT (PM)

Qualys Patch Management (PM) will allow organizations to assess the hosts and common applications against the latest patch levels, and update vulnerable libraries and database applications to ensure they are protected against exploitation in a secure, restricted way, allowing deployment of the latest patches on the assets.

WAF QUALYS WEB APPLICATION FIREWALL (WAF)

Qualys Web Application Firewall (WAF) terminates http/s traffic towards web applications, using virtual, full-proxy architectured appliances that communicate with the Qualys Cloud Platform. Thanks to a powerful DAG oriented logic programmed by tailored rulesets, WAF protects live apps against malicious transactions and load-balances legitimate server-side traffic. The integration with WAS provides powerful mitigation tools, including:

- Virtual patching, which, with one click, provides the ability to prevent confirmed vulnerabilities from being exploited
- ScanTrust, for scanning apps through the WAF in order to assess them and their associated policy
- The ability to map front-end site trees based on active and passive discoveries, to better understand the application and drive decisions

In addition, users can write their own genuine, flexible rules, to adapt transactions in a DevOps manner, and manage them all through a “top-to-bottom” custom ruleset attached to the application. In summary, Qualys’ unique solution aspires to facilitate the SDLC.

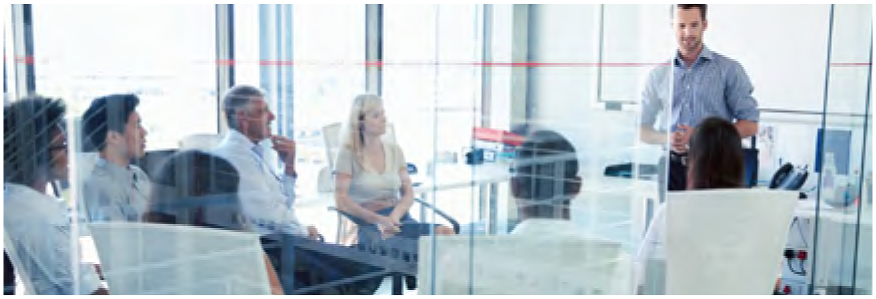
CSC 19

Incident Response and 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.

Organizations must assume that at some point they will have to deal with an attack that successfully breaches their defenses.

Organizations must assume that at some point they will have to deal with an attack that successfully breaches their defenses. That's why they need to have a plan in place to respond and manage such an incident. The plan should include details on procedures, reporting, data collection, management responsibility, legal protocols, and communications strategy. That way the organization will be able to understand, manage, and recover. Lacking an incident response plan could result in an attack going undetected or in a response that's not effective.



CIS recommendations include:

- ✓ Ensure that there are written incident response procedures that include a definition of personnel roles for handling incidents. The procedures should define the phases of incident handling.
- ✓ Assign job titles and duties for handling computer and network incidents to specific individuals.
- ✓ Define management personnel who will support the incident handling process by acting in key decision-making roles.

How Qualys Can Help

FIM QUALYS FILE INTEGRITY MONITORING (FIM)

Qualys File Integrity Monitoring (FIM) monitors and tracks changes to critical files, including important information about security settings, attributes, and the processes involved in the change. This data is critical to helping you detect and identify critical changes and possible security incidents, but can also be priceless when investigating a breach. Centrally-logged change details can be searched quickly to help responders identify the breadth and depth of an attack and possibly uncover collateral damage inflicted during a breach. In the future, Qualys FIM will help speed recovery with ‘self-healing’ features that can roll back changes to critical files.

IOC QUALYS INDICATION OF COMPROMISE (IOC)

Qualys Indication of Compromise (IOC) can continuously monitor assets to detect suspicious activity, flagging telemetry data that could indicate malicious activity on the hosts. In the future, Qualys IOC will auto remediate infected assets by killing the malicious processes.

PM **UPCOMING -** QUALYS PATCH MANAGEMENT (PM)

Qualys Patch Management (PM) will allow organizations to quickly deploy the latest patches, which can speed up recovery and prevent repeat attacks during the incident response process.

Qualys PC data can be leveraged during incident response to find systems with misconfigurations, new or changed services, changes to configuration, permissions, user accounts, and a host of other critical data points that are valuable during the response process. An ad-hoc query tool is on the horizon that will allow responders and IT to find systems with similar issues, which can help identify the breadth and scope of internal or external attacker’s changes to system settings on compromised hosts.

CSC 20

Penetration Tests and Red Team Exercises

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

To determine how effective your security strategies and practices really are you need to subject your defenses to stringent tests that mimic real-world attacks via penetration tests and red team exercises.

CIS recommendations include:

- ✓ Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully. Penetration testing should occur from outside the network perimeter as well as from within its boundaries.
- ✓ Any user or system accounts used to perform penetration testing should be controlled and monitored to make sure they are only being used for legitimate purposes, and are removed or restored to normal function after testing is over.
- ✓ Perform periodic Red Team exercises to test organizational readiness to identify and stop attacks or to respond quickly and effectively.

How Qualys Can Help

VM CM TP QUALYS VULNERABILITY MANAGEMENT (VM CONTINUOUS MONITORING (CM) AND THREAT PROTECTION (TP)

Qualys Vulnerability Management (VM), Continuous Monitoring (CM) and Threat Protection (TP) allow customers to continuously assess and report on the latest evolving vulnerabilities, including zero-day vulnerabilities. TP continuously correlates external threat information against your vulnerabilities and IT asset inventory, leveraging Qualys Cloud Platform's robust back-end engine to automate this large-scale and intensive data analysis process. TP's Live Threat Intelligence Feed displays the latest vulnerability disclosures and maps them to your impacted IT assets. TP can also provide direct links to exploit code for discovered vulnerabilities, helping security teams perform thorough penetration testing.

VM QUALYS VULNERABILITY MANAGEMENT (VM)

Qualys Vulnerability Management (VM) is widely used by consultants and pen-testers to perform network mapping and identify vulnerabilities. It can be leveraged internally using your scanner and agent deployments. Qulays Consultant licenses and offline scanner capabilities can also be used in limited and special engagements.

PC QUALYS POLICY COMPLIANCE (PC)

Qualys Policy Compliance (PC) provides control assessment data that can supplement vulnerability details allowing pen testers more information to dig deeper into an environment.

Born in the cloud, with a fresh approach to security

Qualys.

About Qualys.

The leading provider of IT security and compliance solutions at your fingertips.

The Qualys Cloud Platform and its integrated apps help businesses 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, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also a founding member of the Cloud Security Alliance (CSA).

Request a full trial (unlimited scope) at qualys.com/trial

Qualys is easy to implement, easy to use, fully scalable – and requires NO infrastructure or software to maintain.

Trusted globally

More than 9,300 global businesses in more than 120 countries trust Qualys to underpin digital transformation for greater agility, better business outcomes, and substantial cost savings.

More than 60% of the Forbes Global 50 rely on Qualys and:

- **9 of the top 10 in Technology**
- **9 of the top 10 in Retail**
- **9 of the top 10 in Biotech**
- **7 of the top 10 in Chemical**
- **7 of the top 10 in Banking**

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions with over 9,300 customers in more than 200 countries, including a majority of each of the Forbes Global 100 and Fortune 100. Qualys helps organizations streamline and consolidate their security and compliance solutions in a single platform and build security into digital transformation initiatives for greater agility, better business outcomes and substantial cost savings. The Qualys Cloud Platform and its integrated Cloud Apps deliver businesses critical intelligence continuously, enabling them to automate the full spectrum of auditing, compliance and protection for IT systems and web applications on premises, on endpoints, and in elastic clouds.

For more information, please visit **qualys.com**

Qualys, Inc.
1600 Bridge Parkway
Redwood City, CA 94065

tel: (650) 801 6100
fax: (650) 801 6101

info@qualys.com