Chillisoft Services Health Check Document for Customers Using Qualys Cybersecurity Services

Overview

This health check document evaluates the implementation, performance, and effectiveness of Qualys cybersecurity services, specifically the Qualys Enterprise TruRisk™ Platform, for a customer as of August 22, 2025. It focuses on asset visibility, vulnerability management, risk prioritization, compliance, and operational efficiency, leveraging information from the Qualys website (https://www.qualys.com/), related web sources, and industry best practices.

Chillisoft (www.chillisoft.net) a specialist technical value-added distributor for Qualys in ANZ has been contracted to provide health check services for all existing and new customers of Qualys in the region utilizing our local Qualys certified engineers. This additional local capability is designed to provide more support for partners and customers of Qualys.

Why Your Business Needs a Qualys Health Check

Your organization relies on Qualys to protect its digital infrastructure, identify vulnerabilities, and ensure compliance. But even the most powerful security platforms require regular tuning to stay effective in a constantly evolving threat landscape.

A Qualys Health Check is your proactive step toward stronger security and smarter operations.

Ensure Full Visibility

Validate that all assets—on-prem, cloud, containers, and endpoints—are being discovered and scanned. A health check ensures your asset inventory is complete, accurate, and dynamically updated.

Optimize Platform Performance

Review scan configurations, appliance health, and authentication records to ensure Qualys is running efficiently. This helps reduce scan failures, improve detection accuracy, and streamline operations.

Strengthen Vulnerability Management

Identify gaps in scan coverage, false positives, and outdated templates. A health check ensures your vulnerability detection is precise, and your remediation workflows are aligned with business priorities.

Maximize Module Usage

From VMDR to Patch Management, WAS, and Policy Compliance—ensure each module is properly configured and delivering value. A health check helps you get the most out of your subscription.

Improve Reporting & Compliance

Ensure dashboards and reports reflect current risk posture and compliance requirements. Whether it's internal audits or regulatory mandates, a health check helps you stay ahead of the curve.

Enhance Integrations & Automation

Validate connections with SIEM, CMDB, ITSM, and other tools. A health check ensures your automation workflows are functioning correctly, reducing manual effort and response time.

Tighten Access Controls

Audit user roles and permissions to prevent privilege creep and ensure accountability. This is key for maintaining governance and meeting compliance standards.

CHILLISOFT
Cybersecurity specialists

Qualys

What is included in your Qualys Health Check?

Platform & Subscription Review

- Confirm active modules (VMDR, PM, WAS, PC, CS, etc.)
- Check license usage vs. entitlements
- Review subscription expiration and renewal dates

Asset Management

- Validate asset groups and tags are up to date
- Ensure dynamic tagging rules are working correctly
- Review asset inventory for stale or duplicate entries
- Confirm proper asset scoping for each business unit

Scanner Appliance Health

- Verify all scanners are online and updated
- Check scanner software version and update if needed
- Review scanner load distribution and performance
- Confirm scanner placement covers all network segments

Authentication Records

- Review and test authentication records (Windows, Unix, DBs, etc.)
- Check for expired or failing credentials
- Validate scope and permissions of authenticated scans

Scan Configuration

- Review scan schedules and frequencies
- Validate scan templates and options profiles
- Ensure proper use of performance settings (e.g., TCP retries, timeout)
- Confirm scan coverage across all critical assets

Vulnerability Management

- Review of recent scan results for anomalies or gaps
- Validate QID coverage for critical vulnerabilities
- Check for false positives and tune detection as needed
- Ensure remediation tickets are being generated and tracked

CHILLISOFT
Cybersecurity specialists

Qualys

Patch Management

- Confirm Patch Management module is properly configured
- Review patch jobs and deployment schedules
- Validate patch detection accuracy and coverage
- Check agent health and connectivity
- Ensure rollback and testing procedures are in place
- Monitor patch success/failure rates and troubleshoot issues

Web Application Scanning (WAS)

- Review list of web applications being scanned
- Validate scan schedules and authentication configurations
- Check for scan errors or incomplete scans
- Review findings for critical vulnerabilities (e.g., SQLi, XSS)
- Confirm proper use of WAS tags and asset groups
- Ensure remediation tracking and retesting workflows are active

Reporting & Dashboards

- Review scheduled reports and recipients
- Validate dashboard widgets reflect current priorities
- Ensure executive and technical reporting needs are met

Integration & Automation

- Confirm integration with SIEM, ITSM, CMDB, etc.
- Review API usage and access controls
- Validate automation workflows (e.g., auto-tagging, ticketing)

User Access & Roles

- Audit user accounts and roles
- Remove inactive or unnecessary accounts
- Validate role-based access controls (RBAC)

Compliance & Policy Checks

- Review compliance scan results
- Validate policy templates and mappings
- Ensure alignment with internal and regulatory standards

General Maintenance

- Check for Qualys platform updates or announcements
- Review logs for errors or warnings
- Document changes and findings from the health check