



# Qualys Policy Compliance

One Platform. One Agent. Complete Compliance.

A single platform and agent that facilitates policy compliance for PCI DSS 4.0, GDPR, HIPAA 2023, CCPA, PSD2, ISO, FINRA, DORA, and many more.

*Qualys Policy Compliance (PC) can enhance Vulnerability Detection & Response (VMDR) to ensure compliance and protect PII and Intellectual Property (IP) from cyber threats.*



Policy Compliance helps ensure audit-ready compliance for regulations including PCI DSS 4.0, GDPR, CCPA, PSD2, HIPAA 2023, DORA, FINRA, and more.

## Audit Ready

Full coverage with 900 pre-configured policies, 20,000 controls, 350 technologies, and 100 frameworks.

## Policy Definition

Fast-track compliance assessments using industry-best practices such as CIS Benchmarks and DISA STIGs.

## Compliance Dashboards

Pre-configured dashboards for compliance mandates such as PCI, HIPAA, CCPA, NYDFS, and many more.

## Lower Costs & Complexities

Scan more systems with less effort and automate remediation to reduce efforts and time.

## Accurate, Prioritized Results

Find and prioritize configuration lapses to help achieve, document, and remain compliant.

## Flexible and Extensible

Share configuration data with VM and GRC applications, IT ticketing, and help desk systems.

## Instant Compliance Visibility

Document and generate proof of compliance with detailed reports for auditors and executives.

## Enhanced Security Posture

Improve security hardening scores from 51% to almost 80%, and MITRE ATT&CK coverage to over 86%.

# A single cloud-native solution to simplify and ensure audit-ready compliance and enhanced security.

Qualys Policy Compliance offers a single cloud platform and agent for enterprises that allows you to interactively set up IT standards for hardening configurations and complying with relevant regulations.

Most organizations must protect personally identifiable information (PII) and intellectual property (IP) to avoid compliance audit failures, brand damage, and litigation.

Security teams often overlook improperly configured IT assets, underestimating their security and compliance risks. In fact, misconfigurations, such as default passwords, improper access control settings, weak encryption configurations, or insecure application deployments are major vectors for breaches. Qualys Policy Compliance automates the process of assessing security configurations, starting with configuring policies.

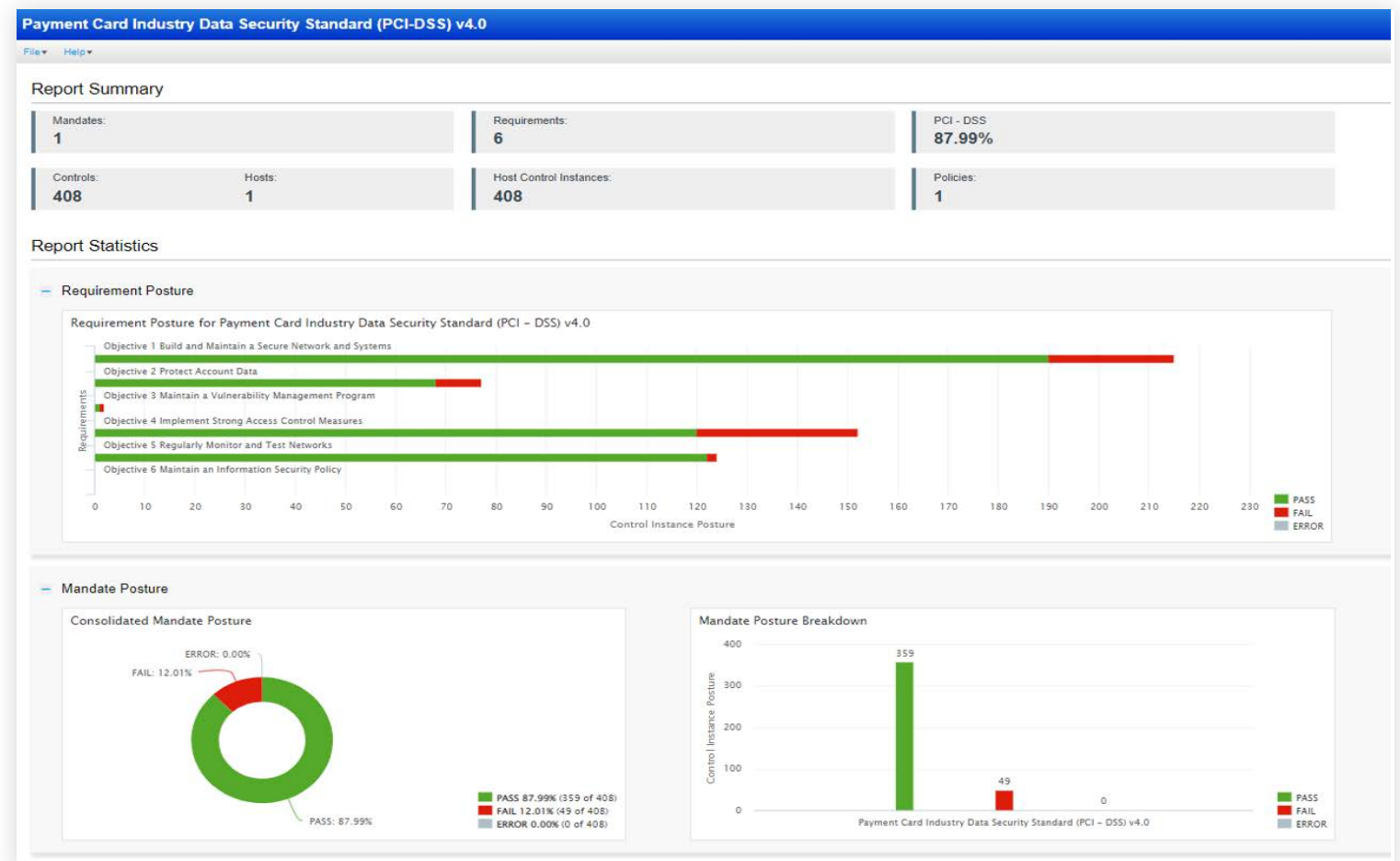
Qualys PC can also improve MITRE ATT&CK® scores from 53 percent to 86 percent and security infrastructure hardening from 51 percent to 79 percent, while reducing total cost of ownership by 43 percent.

Many organizations are governed by various regulations such as GDPR, FINRA, PSD2, HIPAA 2023, PCI DSS 4.0, etc. U.S. State civil codes also trigger penalties for exposing PII and IP.

Regulated firms risk fines and remediation costs for non-compliance, with average costs soaring to \$15 million. Many companies also struggle to implement CIS, NIST, or similar frameworks, which often underscore Written Information Security Policies (WISP) examined by auditors.

Qualys Policy Compliance can enhance any Vulnerability Management solution to help prevent security breaches and audit failures that can lead to serious consequences. Qualys PC automates the labor-intensive process of checking settings on each machine in your environment. By helping you identify violations quickly, before they get out of hand, Qualys PC makes remediation efforts more predictable.

## PCI DSS 4.0 Dashboard



### KEY BENEFITS



#### Cloud Native

Everything is in the cloud and ready to run.



#### Centralized Compliance

Visualize all compliance and security information and assets in one place.



#### Continuous Compliance and Application Security

Start and stay secure and compliant across your entire global infrastructure whether on premises or in the cloud.



#### Improve Security Posture and Hardening

Improve security hardening scores from 51% to almost 80%, and MITRE ATT&CK coverage to over 86%.

### DISCOVER

- ✓ Compliance data available via ad hoc search queries, customized dashboards, and reports.
- ✓ Define configuration policies required for different environments and assets; draw from a library of policies certified by CIS.
- ✓ Manage and build asset inventories required by security standards, including CISA, PCI DSS, FedRAMP, NIST, and SOC 2.
- ✓ 30% improvement in finding previously unknown middleware and databases.

### ASSESS

- ✓ Test controls immediately without rescanning or reporting, create custom controls without writing code or scripts.
- ✓ See how controls relate to critical frameworks and regulations.
- ✓ Select from a rich library of controls, operating systems, network devices, databases, and server applications.

### PRIORITIZE

- ✓ Audit ready for 900 pre-configured policies, 20,000 compliance controls, 350 advanced technologies, and 100 regulatory frameworks.
- ✓ Create custom policies via an interactive web-based editor, add your own policies with an easy to use web-based policy editor.
- ✓ Manage exceptions via a documented approvals process; ensure that audits will show compliance, not uncover violations.

### DEFEND

- ✓ Track compliance metrics across policies, technologies and assets.
- ✓ Document that policies are followed and lapses are fixed, enable data-driven risk and compliance management.
- ✓ Improve MITRE ATT&CK coverage from 53% with Vulnerability Management alone to 86% with VM and PC.
- ✓ Improve average security hardening scores from 51% with Security Configuration Assessment to almost 80%.

### REMEDiate

- ✓ View remediation information in reports, generate mandate-based reports to view your compliance posture.
- ✓ Automate remediation with out-of-the-box scripts & customization.
- ✓ Validate compliance for auditors and stakeholders.
- ✓ Average reduction of 30 days for misconfiguration remediation.

