Measuring, Communicating and Eliminating Compliance Risk Continuously

Qualys®

Enterprise TruRisk™ Platform

Measure, communicate, and eliminate cyber risk.

De-risk your business.

Challenges in measuring Compliance Risk

70% of firms need to comply with **5+** frameworks and regulation standards

Top Compliance Requirements we are failing to measure

18.5%
Inventory of system components

23.7%
Vulnerability Management

16.2%
Patch Management

9.8%
File Integrity Monitoring

19.0%
Configuration Management

NIST 800-53 ISO FedRAMP GDPR PCI HIPAA

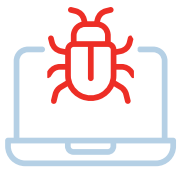
Qualys.

Source: Verizon Payment Security Report

Challenge of measuring exact Compliance Surface

Inability to show Compliance for critical assets

Unknown web servers



Unknown middleware

You can't assess and communicate Compliance Risk of what you don't know

Qualys.

86%

of the data breaches target Web Servers and Middleware

32%

of these mission critical assets are not assessed for Compliance

A clear recipe for Compliance Failures if auditors discover it

Source: 2023 State of the Internet Report

Challenges of Communicating Compliance Risk

Compliance risk communication is multifold. Need to communicate at multiple levels

CISO/Executives

How do I measure the Risk?

- Overall Compliance Posture
- Risk of Compliance Audit failures
- Is Compliance risk reducing?

Management

How do I measure and communicate the Risk?

- Compliance coverage
- Each requirement wise failures
- Unified Compliance reports

Security Analysts/IT

How can I eliminate the risk?

- Granular visibility into misconfigurations
- Password Policies, Access Controls
- Preventing misconfigurations

Qualys.

Compliance is not just about scanning. It is more about mapping and reporting for diverse compliance standards.

Qualys.

The Solution

Qualys.

Measure

Communicate

Eliminate

Configuration Management

File Integrity Monitoring

Unified Reporting

Auto Remediation

20k
Security Controls

65
Regulations
Frameworks

997
Library policies

350
Technologies

PCI DSS 4.0 FIM Requirements

10.2.2 FIM events must have who, what, when and where details
10.3.4 Alert when existing log data is changed
10.4.1.1 New Requirement: Automated audit log reviews
10.5.1 Data retention for at least 12 months
10.7.2 New Requirement: Alert when FIM fails to work
11.5.2 FIM is deployed

Continuous Compliance

Qualys.

Identify and Classify Your Assets

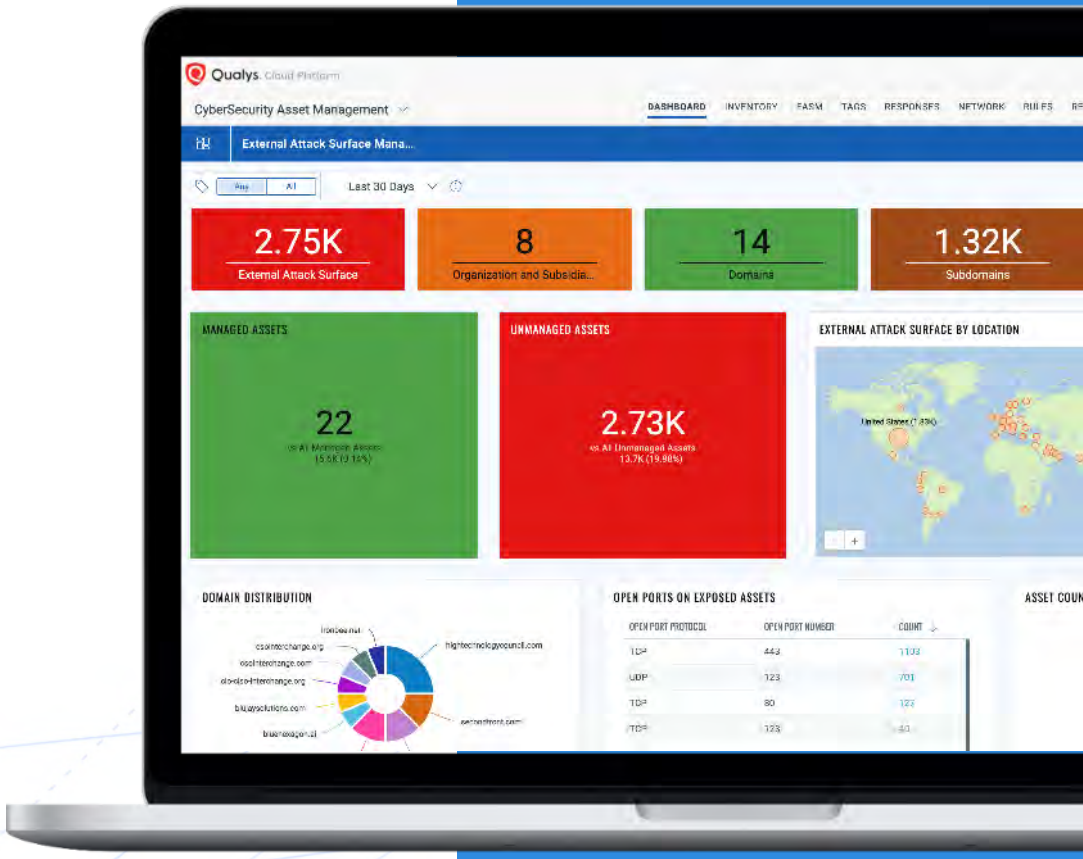
Measure risk by knowing your Compliance Surface

Identify assets with EOL/EOS software

Assets exposed to Shodan

Auto discover web servers, middleware

Classify mission critical assets for PCI compliance



Qualys.

Risk Based Prioritization

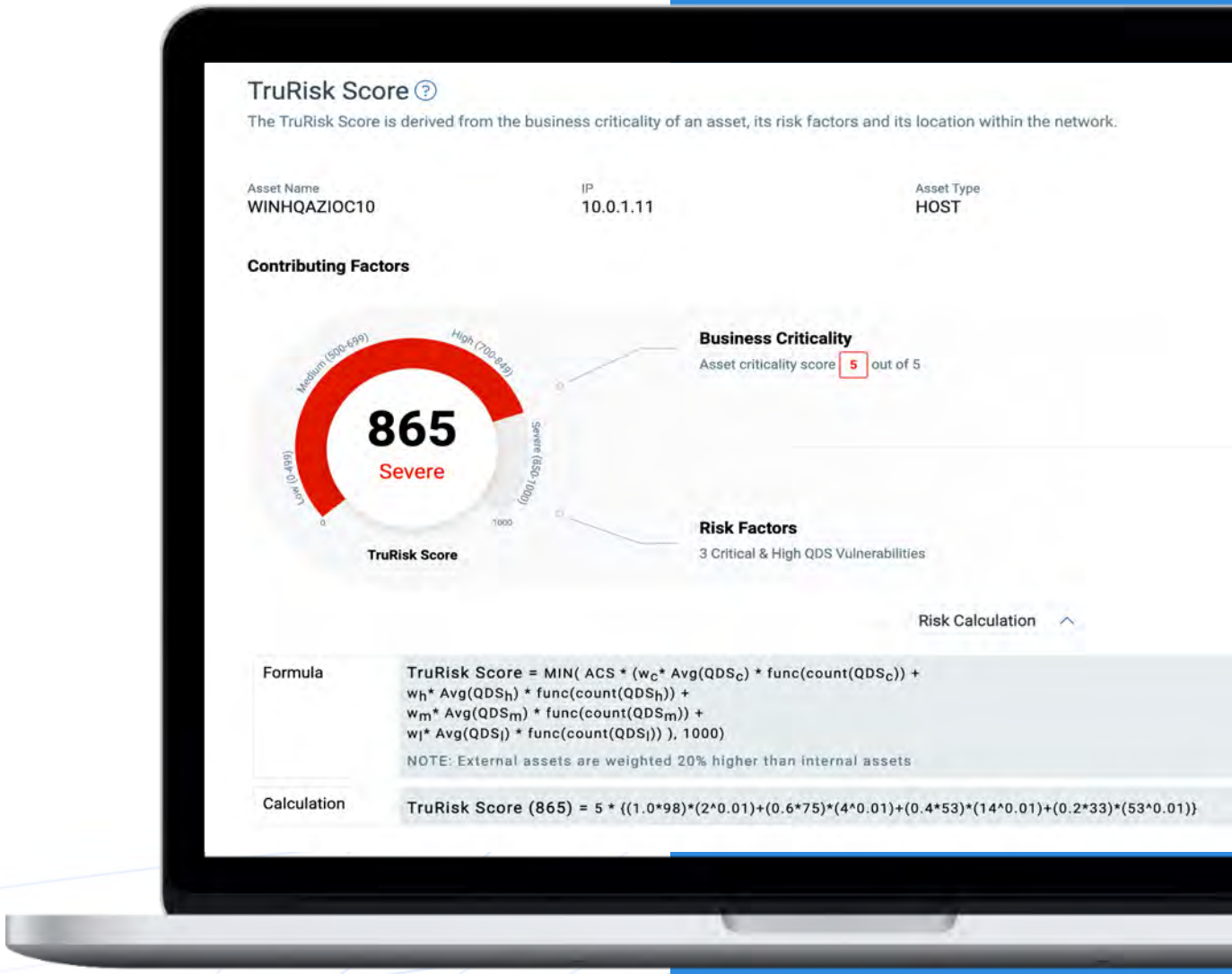
Measure the Risk

TruRisk

TruRisk integration

Prioritize risk of your misconfigurations

- Asset criticality
- MITRE ATT&CK mapping
- Control Severity
- Ransomware Exposure

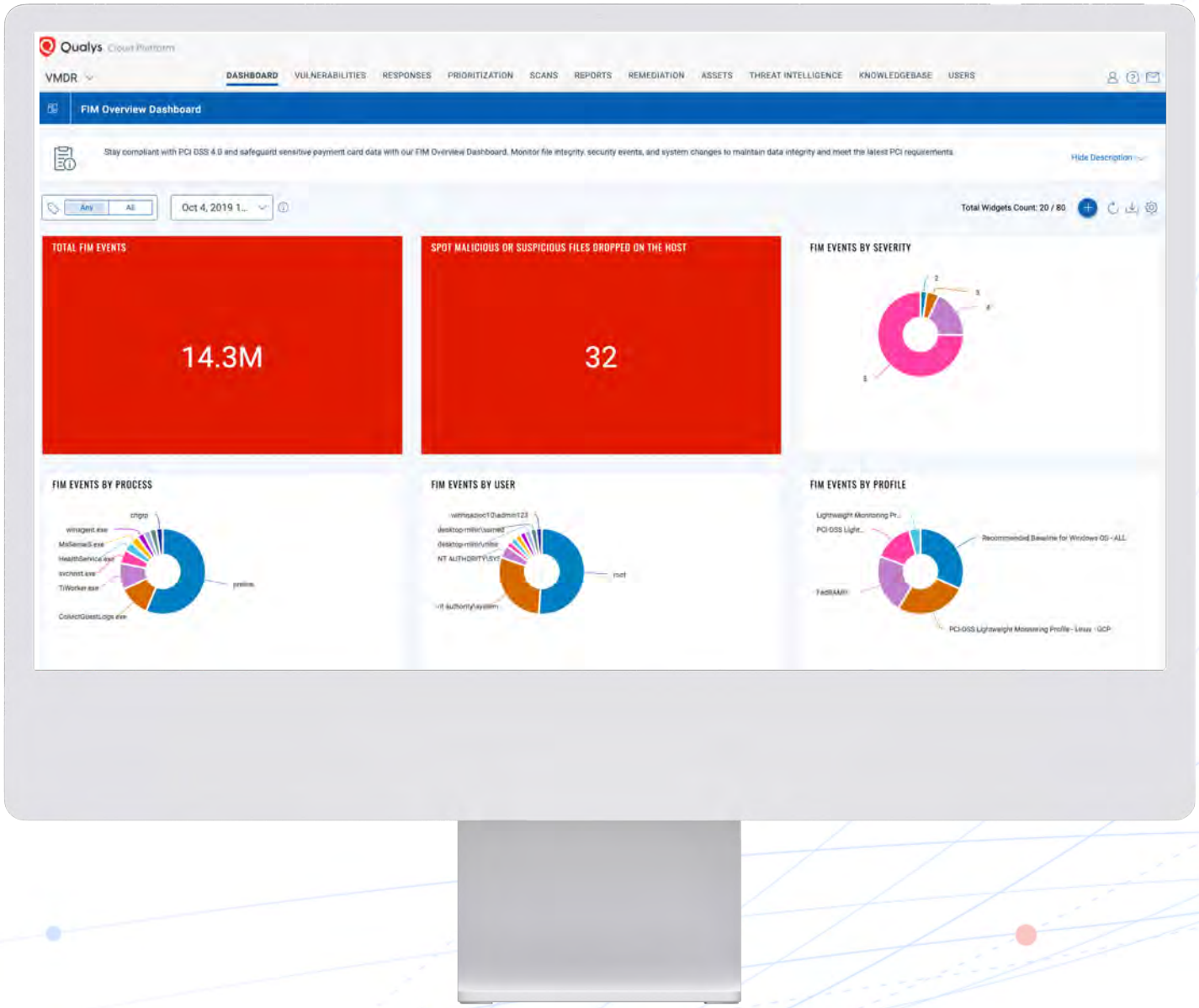


Qualys.

File Integrity Monitoring

Measuring the compliance for PCI 4.0, HIPAA, NIST SI-7

- **Full coverage for PCI DSS 4.0** and other compliance regulations
- Advanced Noise Cancellation
- Inbuilt Threat Intelligence to Detect Malicious or Suspicious Hashes
- Same Agent

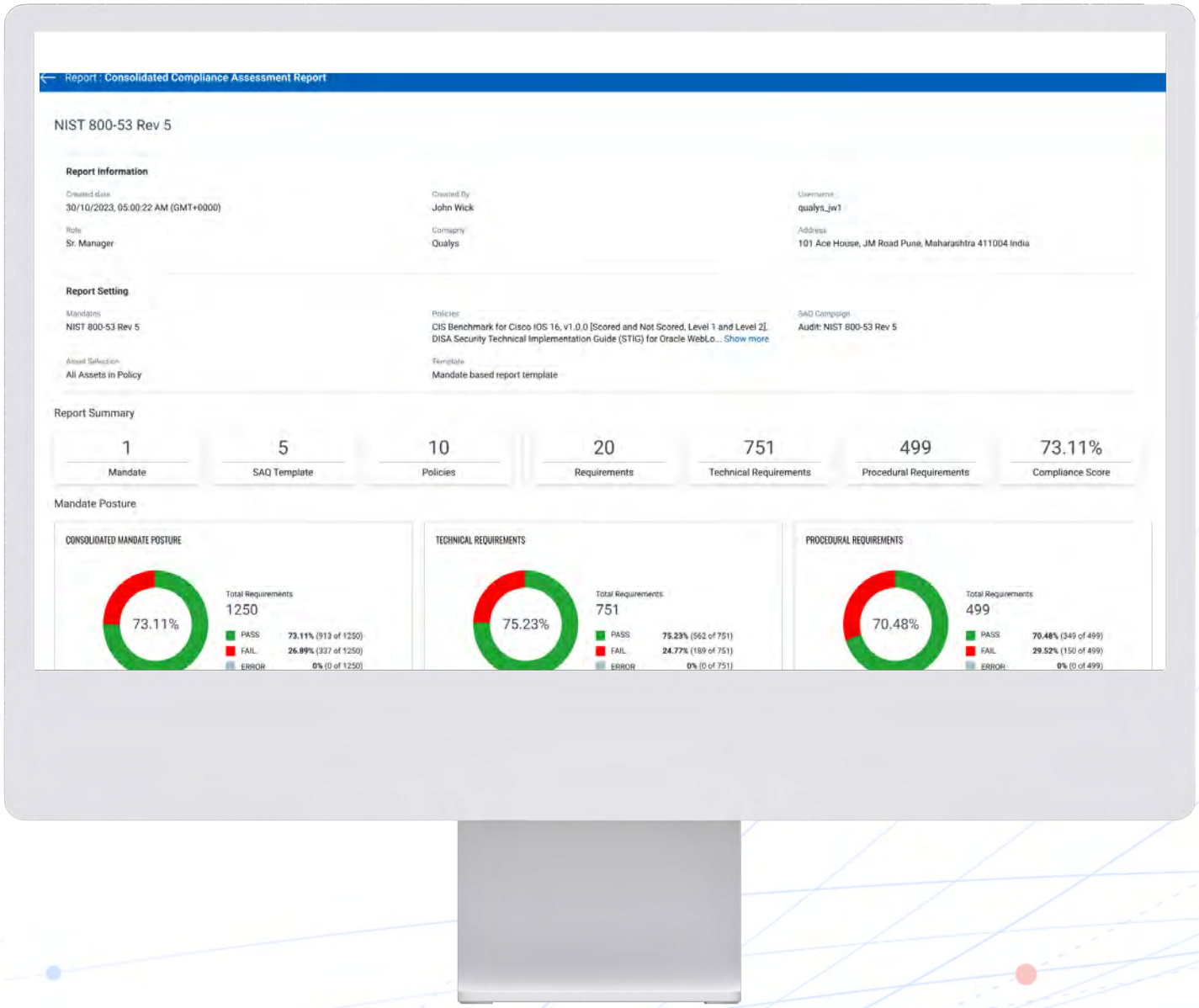


Qualys.

Communicate Compliance to your auditors

Out-of-the-box reporting for most failed compliance requirements

- Compliance reporting with auto cross mapping to 60+ security benchmarks and frameworks including CIS, DISA, NIST, PCI DSS
- FIM reports for PCI 4.0
- Unified assessment and tracking of Technical and Procedural controls
- Always Audit Ready



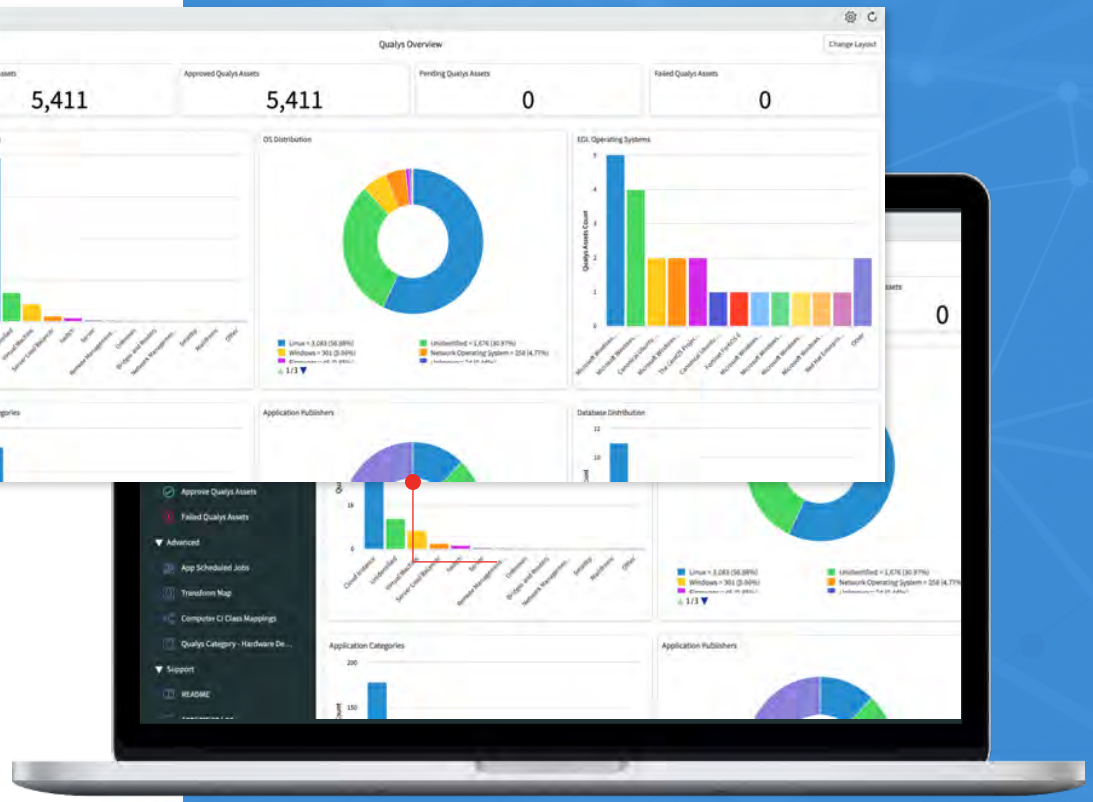
Qualys.

Automate ITSM Workflows

Communicate the Compliance Risk

Close the IT-Security gap

- Automatically create ServiceNow tickets remediate misconfigurations
- Communicate compliance risk to your GRC tools
- Automatically close out tasks once misconfigurations are resolved



Qualys.

Start Compliant, Stay Compliant

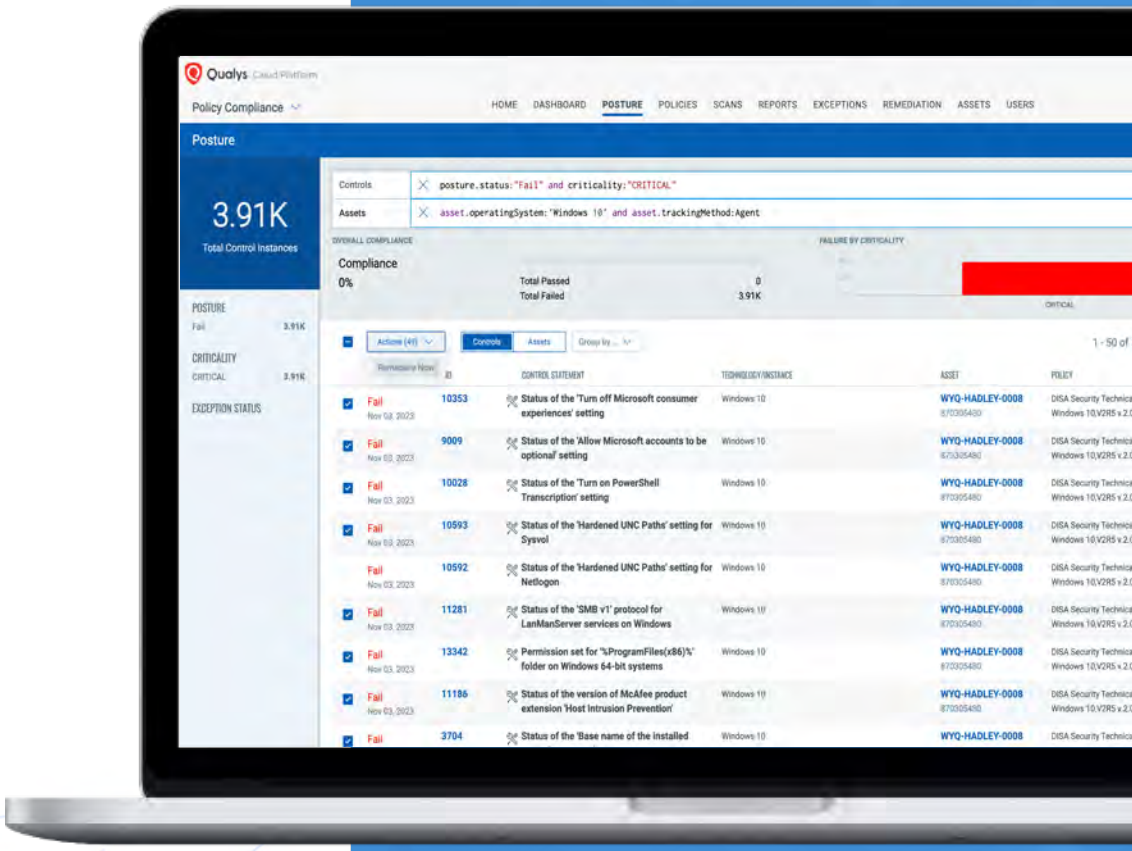
Eliminate the Risk from initial stages

Pre-defined Library for PCI 4.0 and NIST in CI/CD

Start being compliant with golden images

Automatically fix compliance failures before non-compliant images roll out in production

Prevent exploits and improve overall compliance posture



Qualys.

Risk Reduction Impact

43% Potential Cost Savings and Risk Reduction

80% Average Compliance Score for customers using Qualys Policy Compliance vs customers just scanning for CIS benchmarks 51%

24% Reduction in compliance fines

Qualys.

Demo

Qualys.

Topics

Continuous Compliance and Cloud

Four Common Trends in PCI Compliance

Continuous Compliance: Four Key Changes for Organizations

Qualys' Vision for PCI DSS 4.0

Qualys.

Source: Qualys Cyber Risk Series


SC
23