

QUALYS GUARD® ENTERPRISE *for Public Sector*

GLOBALLY DEPLOYABLE, SCALABLE FISMA AND POLICY COMPLIANCE MANAGEMENT

QualysGuard Enterprise enables Federal and State government agencies to reduce risk and manage their FISMA and Certification & Accreditation (C&A) and policy compliance processes.

QualysGuard provides comprehensive risk and policy compliance management, monitoring and reporting in one solution. QualysGuard automates the vulnerability scanning, management and policy compliance required for FISMA and C&A compliance by providing asset discovery and mapping, FIPS asset and system classification, vulnerability assessment reporting and plan of action and milestone (POA&M) tracking according to risk classification and system boundaries.

In preparing for FISMA compliance, agency heads, in conjunction with CIOs and CISOs, can use QualysGuard to support the eight broad FISMA reporting categories:

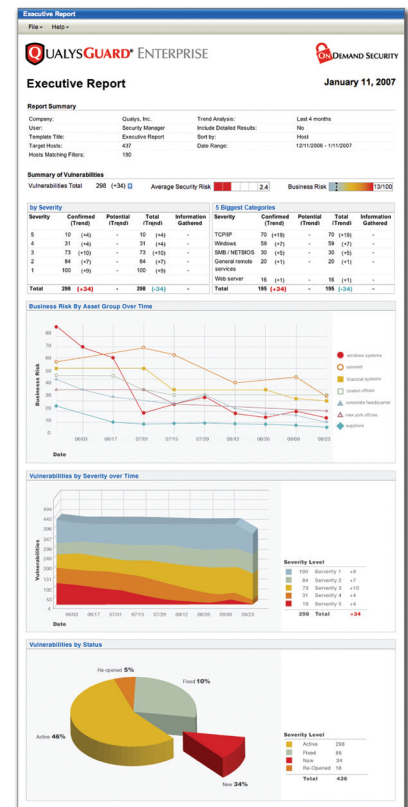
- | | |
|---------------------------------------|--|
| 1. Risk Assessment | 5. Annual Security Testing |
| 2. Policies and Procedures | 6. Remediation Procedures |
| 3. Security Plans | 7. Incident Response Procedures |
| 4. Security Awareness Training | 8. Contingency Plans |

QualysGuard Enterprise is ideal for large, distributed agencies with:

- Global complex, segmented and remote networks with thousands of devices
- Numerous departmental users requiring role-based access to vulnerability, compliance and POA&M data
- Agencies requiring consolidated technical and executive-level reporting on compliance

Benefits of QualysGuard Enterprise for Government Agencies:

- Automatically and rapidly identify, visualize and organize system assets into Department, Agency, Bureau and C&A system defined Asset Groups
- Manage risk by automating vulnerability identification and prioritization of remediation based on FIPS 199 system classifications and risk profiles
- Document regulatory compliance via automated agent-less auditing, tamper resistant audit trails and the certainty that comes with required third-party assessments
- Unprecedented scalability makes it ideal for large, distributed organizations
- On demand SaaS technology offers significant economic advantages with no capital expenditures, extra human resources or infrastructure to deploy and manage



QualysGuard Enterprise Features:

Centralized Vulnerability Management

- Eliminate point in time security testing and evaluation (ST&E) results and create continuously managed technical findings from your certification and accreditation (C&A) process
- Automatic and centralized reporting of distributed scans results from globally diverse environments
- Consolidated administration of both internal and external (perimeter) findings
- Create, track and trend on progress against POA&M reports for on demand reporting by business unit for executives and managers
- Executive Dashboard and reporting with scorecard compliance reporting
- Remediation reporting: ticket trending by asset group, user and vulnerability
- Authorized role based user access from any location
- Export reports to HTML, MHT, PDF, CSV and XML formats

FISMA Policy Compliance

- Create a true FISMA continuous monitoring solution for enterprise security risk exposure
- Measure time to remediate security risk by FIPS classification as well as C&A system boundaries
- Provide continuous trending of security risk, vulnerability exposure and policy compliance across enterprise, by system or by FIPS classification
- Provide automated alerting based on asset and system risk scores

Automation

- Automatically provide FISMA required continuous monitoring through scheduled vulnerability, policy and asset discovery scans
- Automated daily updates to vulnerability KnowledgeBase
- Automated report generation by system owner, executive or IG resources
- Automated remediation ticket generation and verification



QualysGuard Scanner Appliances deliver an easy-to-use scanning infrastructure for distributed networks that can be deployed in minutes.

Accuracy

- Inference-based scanning engine with non-intrusive and accurate scanning techniques
- Comprehensive vulnerability KnowledgeBase incorporates thousands of unique checks

- Trusted, third-party certification of network security with tamper resistant audit trails
- Internal and external scanning provides a 360-degree view of department and agency as well as system boundary vulnerability exposure
- Both un-trusted and authenticated scanning capabilities
- Configurable scans for customized audits
- Unique fingerprints for over 500 operating systems, applications and protocols

Scalability/Deployability

- On demand SaaS technology allows users to scan globally with no additional infrastructure
- Fast scanning through load balancing of scanner appliances
- User definable department, agency, and bureau units and asset groups that tie into department and system categorization
- End-to-end encryption of vulnerability data
- Hierarchical role-based user access controls allow delegation of responsibilities to reflect organizational structure
- Policy-based remediation workflow management with automatic trouble ticket creation and assignment

Interoperability

- Extensible XML API
- Security compliance SDK and application library
- Out-of-the-box integration with leading SIM solutions
- Integration with helpdesk systems
- Integration with Patch Management systems for auto-remediation capabilities
- Integration with leading Network Admission Control vendors including Cisco NAC
- Industry standard support for vulnerability scoring with Common Vulnerability Scoring System (CVSS)
- Industry standard support for the addition of custom detections using Open Vulnerability Assessment Language (OVAL)

Support/Maintenance

- 24x7x365 live customer support
- Daily signature updates and feature enhancements are completed automatically, transparent to the user
- Ongoing Web-based customer training
- Technical training and certification workshops

“With QualysGuard, we know that our systems are highly secure and up-to-date. The service also validates that our internal security policies, and regulatory mandates, are enforced.”

Manager, Network Services Headquarters
U.S. Marine Corps – Personal and Family Readiness Division (MRI)

“Qualys has helped us reduce vulnerabilities, especially by identifying where automated patch processes are not working.”

Chief Information Officer
Florida Department of Health



Qualys Wins an Unprecedented 5 SC Magazine Awards

SC Magazine Awards recognize distinguished vendors based on readers choice. Qualys was awarded:

- Best Vulnerability Assessment & Remediation Solution
- Best Enterprise Security Solution
- Best SME Security Solution
- Best European Security Company
- Best European Security Solution



USA – Qualys, Inc. • 1600 Bridge Parkway, Redwood Shores, CA 94065 • T: 1 (650) 801 6100 • sales@qualys.com
UK – Qualys, Ltd. • 224 Berwick Avenue, Slough, Berkshire, SL1 4QT • T: +44 (0) 1753 872101
Germany – Qualys GmbH • München Airport, Terminalstrasse Mitte 18, 85356 München • T: +49 (0) 89 97007 146
France – Qualys Technologies • Maison de la Défense, 7 Place de la Défense, 92400 Courbevoie • T: +33 (0) 1 41 97 35 70
Japan – Qualys Japan K.K. • Pacific Century Place 8F, 1-11-1 Marunouchi, Chiyoda-ku, 100-6208 Tokyo • T: +81 3 6860 8296
Hong Kong – Qualys • 2/F, Shui On Centre, 6-8 Harbour Road, Wanchai, Hong Kong • T: +81 3 6860 8296

