Most vulnerability management solutions do little to help security leaders put vulnerability and risk information in the context of business. Saddled with volumes of rigid data and static reports, the security team is left to manually discern real threats and determine how to act upon them. At Symantec, we believe that security professionals deserve more from their vulnerability management solutions. That’s why we deliver vulnerability data in the proper context.

Control Compliance Suite Vulnerability Manager: The Context-Aware Vulnerability Management Solution

Symantec® Control Compliance Suite Vulnerability Manager (CCSVM) is the only vulnerability management solution designed from the ground up to provide organizations with context-aware vulnerability assessment and risk analysis. Its results-driven architecture works with users to proactively identify security exposures, analyze business impact, and plan and conduct remediation across network, web, mobile, cloud, virtual, and IoT infrastructure.

- Discover network, web, mobile, cloud, virtual, and IoT infrastructure.
- Profile asset configuration and risk potential.
- Pinpoint vulnerabilities, malware and attacks.
- Analyze threat potential, return on remediation and more.
- Isolate high-risk assets through advanced threat analytics.
- Trigger remediation through integration with 3rd party systems.
- Report on vulnerabilities, compliance, benchmarks, etc.
- Protect endpoints against client-side attacks.

**Figure 1.** CCSVM enables you to understand and prioritize risk in the context of your business via the centralized Control Compliance Suite management, reporting and analytics console.
Key Capabilities

ZERO-GAP COVERAGE
Able to discover and assess any IT resource, CCSVM offers zero-gap coverage of the largest, most diverse IT environments. Agentless and agent-based scanning protects both online and offline assets.

UNMATCHED REPORTING
With the most powerful reporting capabilities in its class, CCSVM makes it easy to make smarter decisions, communicate risk, and report remediation progress to executives and compliance auditors.

ADVANCED THREAT ANALYTICS
CCSVM discovers data breach threats typically missed by other vulnerability solutions. The solution pinpoints specific, high-risk users and assets by correlating vulnerability and threat data from a variety of Symantec and third-party solutions.

EXTENSIVE COMPLIANCE COVERAGE
Reporting for COBIT, GLBA, HIPAA, HITRUST, ISO, ITIL, NERC-FERC, NIST, PCI, SOX, and many more government & industry regulations.

ENTERPRISE SCALABILITY AND FLEXIBILITY
CCSVM’s multi-tier architecture is designed for simple deployment and management of networks with multiple firewalls, IDS/IPS, VLANS and disparate locations.

Control Compliance Suite Vulnerability Manager Threat and Vulnerability Intelligence
CCSVM provides centralized management, policy, reporting, and analytics for vulnerability management solutions. Capabilities include:

- Centralized solution management and control via common dashboards
- Asset discovery, profiling and grouping
- Reporting and analytics
- Workflow and ticketing

UNMATCHED REPORTING & ANALYTICS

- Results-Driven Architecture
  Tailor scans to specific reporting and compliance requirements.

- Advanced Threat Analytics
  Detect critical threats thru volumes of data.
Control Compliance Suite Vulnerability Manager
Intelligently Identify and Prioritize the Remediation of System Vulnerabilities

Data Sheet

- Resource Planning
  Run what-if scenarios and team capacity analyses to plan resource allocation.

- 100+ Actionable Reports
  Communicate with technical and non-technical audiences.

- Compliance Reporting
  COBIT, GLBA, HIPAA, HITRUST, ISO-27002, ITIL, MASS 201, NERC-FERC, NIST, PCI, SOX and more.

- Advanced Threat Intelligence
  Based on asset scoring, security research, exploit databases, exploitability, NSRL, CVSS v3, CWE, and more.

- Trends, Deltas and Heat Maps
  Share progress with executives, compliance auditors and others.

- SLA Compliance Reports
  Measure threat severity level against dynamic asset groupings.

- Pivot Grid Ad-Hoc Reporting
  Create custom reports.

- Third-Party Integration
  SIEM, GRC, NMS and help desk integration

MAXIMUM FLEXIBILITY

- Flexible Deployment
  Deploy software, appliances and/or virtual machines.

- Centralized Dashboards
  Consolidate enterprise-wide activities.

- Integrated Data Warehouse
  Analyze historical data over time.

- Role-Based Access
  Provide permissioned access to view, assess and report on data.

- Effortless Updates and Upgrades
  Expand capabilities via license updates.
ZERO-GAP COVERAGE

- **Vulnerability Assessment**
  Flag vulnerabilities, attacks, and malware by asset for a complete view of risk.

- **Comprehensive Discovery**
  Locate network (local and remote), web, mobile, cloud, virtual and IoT assets.

- **Asset Profiling**
  Gather information including IP, DNS, OS, MAC address, ports, services, software, processes, hardware, event logs and more.

- **Asset Smart Groups**
  Group, assess, and report on assets by IP range, naming convention, OS, domain, applications, business function and more.

- **Asset Context Awareness**
  Evaluate risk based on damage potential or target distribution, plus confidentiality, integrity and availability requirements.

- **Smart Credentials**
  Automatically scan targets using the highest privilege level.

- **Asset Risk Analysis**
  Compare asset risk levels with custom Threat Risk and Exposure Risk scoring.

- **Cloud Scanning**
  Scan online & offline Amazon®, GoGrid®, Google®, IBM®, Rackspace® & VMware®.

- **VMware Verified**
  Scan virtual environments requiring PCI and HIPAA compliance.

- **Patch Management**
  Remediate with patch management using ticketing tools and integrations for Microsoft and third-party applications.

- **Scheduling and Alerts**
  Schedule scans and configure email alerts.
ENTERPRISE SCALABILITY

- **N-Tier, Multitenant Architecture**
  Gain maximum scalability and control.

- **Scan Engine Pooling**
  Combine scan engines, each able to scan a Class-A network in under 15 minutes.

- **Retina Protection Agent**
  Local scanning, zero-day monitoring, and intrusion prevention for offline devices.

- **Local and Remote Scanning**
  Cover segregated, firewalled and disparate infrastructure.
Control Compliance Suite Vulnerability Manager
Intelligently Identify and Prioritize the Remediation of System Vulnerabilities

More Information
Visit our website
http://go.symantec.com/ccs

To speak with a Product Specialist in the U.S.
Call toll-free 1 (800) 745 6054

To speak with a Product Specialist outside the U.S.
For specific country offices and contact numbers, please visit our website.

About Symantec
Symantec Corporation (NASDAQ: SYMC), the world’s leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec’s Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world’s largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com