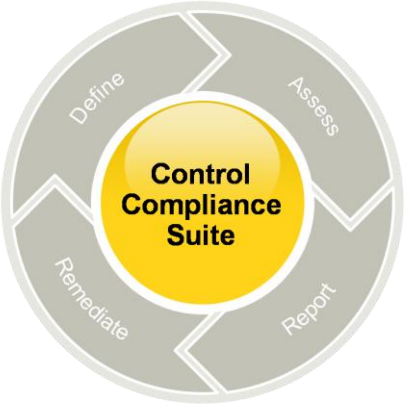
Data Sheet: Compliance and Security Management

Symantec™ Control Compliance Suite 9.0

Automates key IT compliance activities including risk assessment, policy management; IT controls assessment and monitoring, remediation, and reporting

Overview

Control Compliance Suite provides end-to-end coverage for the IT compliance lifecycle, including policy management, technical and procedural controls assessment, reporting and remediation. CCS provides the most comprehensive view of risk and compliance posture with a combination of point-in-time controls assessment and real-time monitoring of risks and threats. CCS is an open architecture that enables integration with business processes and other external solutions.



The need to automate key IT compliance processes

Today, the complexity of ensuring compliance and strong IT governance in an organization is made more difficult by the variety of security issues that must be monitored and the need to comply with multiple external mandates. Recent research indicates that companies investing in one-off solutions for each compliance mandate they face will spend significantly more on IT compliance than those that develop a single solution to manage multiple mandates.

The action most responsible for best-in-class compliance results is the frequent measurement of IT-based controls, policies, and audit results. Industry leaders are monitoring, measuring, and reporting on these once every 21 days and are conducting internal audit and IT security monitoring eight times more frequently than are industry laggards.1

Unfortunately, the majority of costs associated with implementing strong IT compliance come from often-repeated, time-consuming processes: creating, defining and distributing policies, tracking exceptions, managing standards, managing entitlements, remediating deviations, and performing both procedural and technical assessments. Thus, the critical need for organizations is finding a way to perform these costly processes more efficiently.

Organizations are struggling not just with maintaining strong IT compliance, but also with understanding what policies and standards they should be implementing. A typical organization is a complex, heterogeneous environment, with a variety of platforms and a diverse set of control objectives. Understanding what is required and how to achieve cost effective, strong IT compliance requires comprehensive intelligence of regulations, frameworks, and the relevant best practices, and the appropriate tools to automate the process.

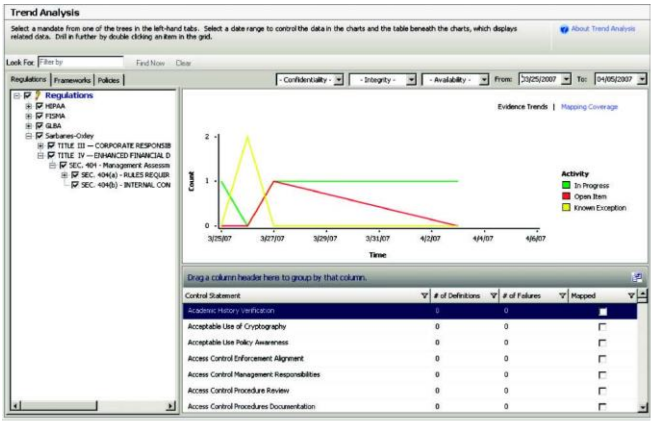
Symantec Control Compliance Suite

The Symantec Control Compliance Suite is an integrated set of technologies that enable the key processes needed to achieve and maintain IT compliance. By providing these technologies in a single solution, Symantec Control Compliance Suite can make the process of compliance easier and more cost-effective for customers.

[1] Improving IT Compliance: 2006 IT Compliance Benchmark Report," June 2006

Policy Manager

The Policy Manager assists with defining and mapping policies to best practices, frameworks, and regulations, and identifies overlaps in control objectives to reduce duplicative assessment efforts. The Policy module also automates the distribution of written policies throughout the organization, tracking end-user policy acceptances and exception requests. The Policy module collects evidence of compliance to control objectives through integration with other Symantec Control Compliance Suite components that provide both procedural and technical assessments, thus enabling analysis and reporting on compliance efforts. In addition, the Policy Module ships with over 125 sample policies and policy templates, and if fully and easily customizable.   Newly enhanced reporting and dashboard capabilities allow more flexibility for distributing information.



Trend Analysis

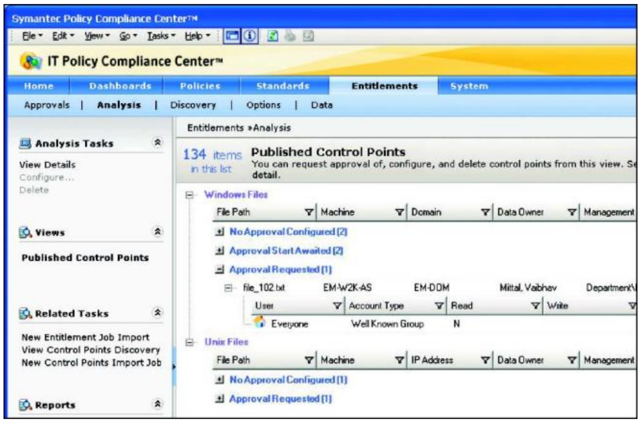
Select a mandate from one of the trees in the left-hand tabs. Select a date range to control the data in the charts and the table beneath the charts, which displays related data. Drill in further by double clicking an item in the grid.

Control Statement	# of Definitions	# of Failures	Mapped
Academic History Verification	0	0	☑
Acceptable Use of Cryptography	0	0	□
Acceptable Use Policy Awareness	0	0	□
Access Control Enforcement Alignment	0	0	□
Access Control Management Responsibilities	0	0	□
Access Control Procedure Review	0	0	□
Access Control Procedures Documentation	0	0	□

Figure 1. Policy Module—trend analysis

Entitlement Manager

The Entitlement manager gathers effective permissions on data from across the enterprise, translates those permissions into a consistent human-readable format, associates management classification to the data, and electronically routes the information to business owners for access approval. Entitlements approvals are tracked and tied to analysis/audit reports as controls evidence.



Symantec Policy Compliance Center™
File
Edit
View
Go
Tasks
Help
IT Policy Compliance Center™
Home
Dashboards
Policies
Standards
Entitlements
System
Approvals | Analysis | Discovery | Options | Data
Analysis Tasks
View Details
Configure...
Delete
Views
Published Control Points
Related Tasks
New Entitlement Job Import
View Control Points Discovery
New Control Points Import Job
Reports

Entitlements »Analysis

134 items in this list

Published Control Points
You can request approval of, configure, and delete control points from this view. Se detail.

Windows Files

File Path	Machine	Domain	Data Owner	Management
No Approval Configured (2)				
Approval Start Awaited (2)				
Approval Requested (1)				
file_102.txt	EM-W2K-AS	EM-DOM	Mittal, Vaibhav	Department\

User	Account Type	Read	Write
Everyone	Well Known Group	N	

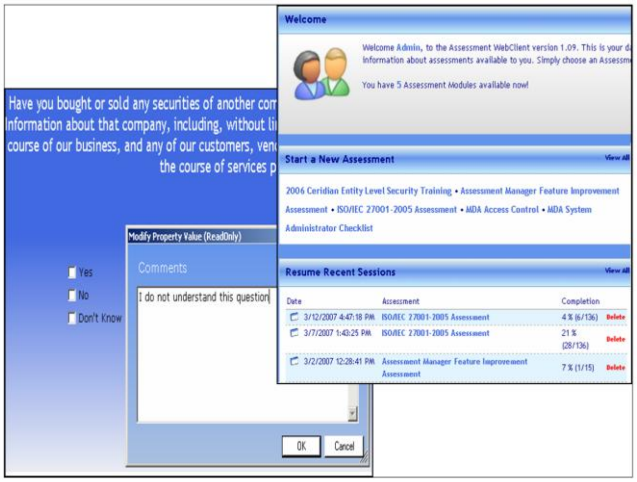
Unix Files

File Path	Machine	IP Address	Data Owner	Management
No Approval Configured (1)				
Approval Requested (1)				

Figure 2. Discovery and configuration of entitlement control points

Response Assessment module

The Response Assessment module automates the assessment of non-programmatic controls. These non-programmatic controls make up the majority of objectives laid out in regulations/frameworks. Organizations often rely on paper-based assessments that are expensive and difficult to manage. RAM manages the manual assessment process from questionnaire creation and distribution to analysis of response data. RAM integrates with Symantec Control Compliance Suite to provide a comprehensive view of both procedural and technical controls, thus ensuring policy coverage.



Have you bought or sold any securities of another com
Information about that company, including, without li
course of our business, and any of our customers, ven
the course of services p

□ Yes
□ No
□ Don't Know

Modify Property Value (ReadOnly)

Comments

I do not understand this question

Welcome

Welcome Admin, to the Assessment WebClient version 1.09. This is your d
information about assessments available to you. Simply choose an Assessm

You have 5 Assessment Modules available now!

Start a New Assessment

2006 Ceridian Entity Level Security Training • Assessment Manager Feature Improvement Assessment • ISO/IEC 27001-2005 Assessment • MDA Access Control • MDA System Administrator Checklist

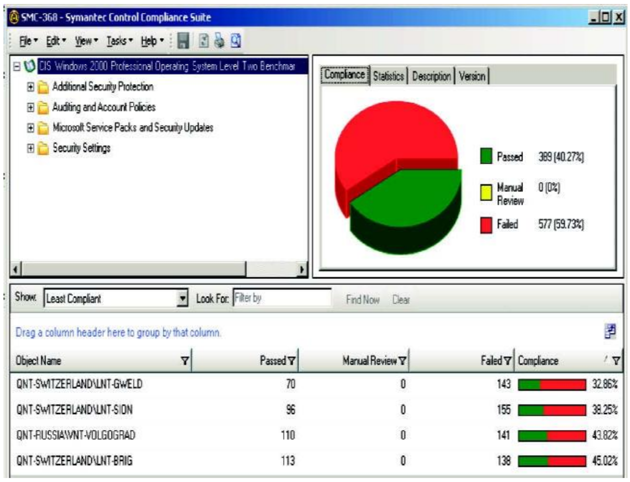
Resume Recent Sessions

Date	Assessment	Completion	
3/12/2007 4:47:18 PM	ISO/IEC 27001-2005 Assessment	4 % (6/136)	Delete
3/7/2007 1:43:25 PM	ISO/IEC 27001-2005 Assessment	21 % (28/136)	Delete
3/2/2007 12:28:41 PM	Assessment Manager Feature Improvement Assessment	7 % (1/15)	Delete

Figure 3. Response Assessment Module

Standards Manager

The Standards module automates the management of deviations from technical standards and makes it possible to remediate misconfigurations. The Standards module provides prepackaged technical standards that granularly define best practices for securing servers and databases and trends compliance to these standards. In addition, the Standards module of the Symantec Control Compliance Suite provides detailed remediation instructions to correct deviations and integrates with existing change control ticketing systems to ensure that changes are made only after appropriate authorization and with proper oversight.



CIS Windows 2000 Professional Operating System Level Two Benchmar
- Additional Security Protection
- Auditing and Account Policies
- Microsoft Service Packs and Security Updates
- Security Settings

🟩	Passed	389 (40.27%)
🟨	Manual Review	0 (0%)
🟥	Failed	577 (59.73%)

Show: Least Compliant Look For: Filter by

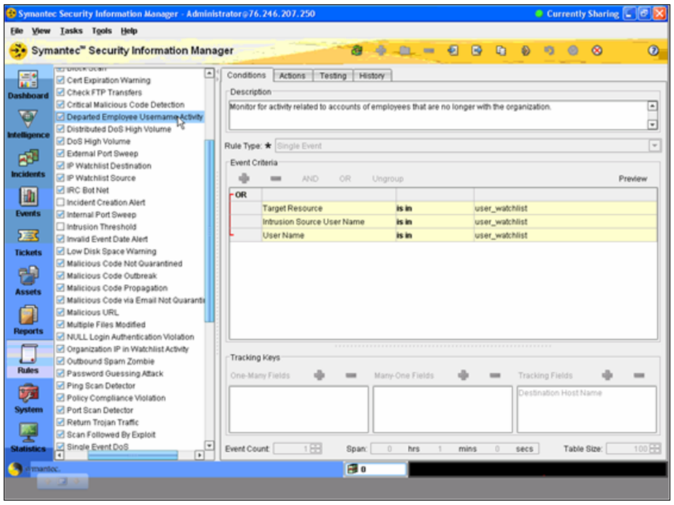
Drag a column header here to group by that column.

Object Name	Passed	Manual Review	Failed	Compliance
QNT-SWITZERLAND\LNT-GWELD	70	0	143	32.86%
QNT-SWITZERLAND\LNT-SION	96	0	155	38.25%
QNT-RUSSIA\WNT-VOLGOGRAD	110	0	141	43.82%
QNT-SWITZERLAND\LNT-BRIG	113	0	138	45.02%

Figure 4. Technical controls assessment and reporting

Security Information Manager

Security Information Manager enables organizations to collect, store, and analyze log data as well as monitor and respond to security events to meet IT risk and compliance requirements. It can collect and normalize a broad scope of event data and correlate the impact of incidents based on the criticality to business operations or level of compliance to various mandates. Incidents are prioritized using its built-in asset management function, which is populated using scanning tools and allows confidentiality, integrity, and response ratings and policies to be assigned to help prioritize incidents.



☑ Cert Expiration Warning
☑ Check FTP Transfers
☑ Critical Malicious Code Detection
☑ Departed Employee Username Activity
☑ Distributed DoS High Volume
☑ DoS High Volume
☑ External Port Sweep
☑ IP Watchlist Destination
☑ IP Watchlist Source
☑ IRC Bot Net
□ Incident Creation Alert
☑ Internal Port Sweep
□ Intrusion Threshold
☑ Invalid Event Date Alert
☑ Low Disk Space Warning
☑ Malicious Code Not Quarantined
☑ Malicious Code Outbreak
☑ Malicious Code Propagation
☑ Malicious Code via Email Not Quaranti
☑ Malicious URL
☑ Multiple Files Modified
☑ NULL Login Authentication Violation
☑ Organization IP in Watchlist Activity
☑ Outbound Spam Zombie
☑ Password Guessing Attack
☑ Ping Scan Detector
☑ Policy Compliance Violation
☑ Port Scan Detector
☑ Return Trojan Traffic
☑ Scan Followed By Exploit
☑ Single Event DoS

Description: Monitor for activity related to accounts of employees that are no longer with the organization.

Rule Type: ★ Single Event

Event Criteria

OR		
Target Resource	is in	user_watchlist
Intrusion Source User Name	is in	user_watchlist
User Name	is in	user_watchlist

Tracking Keys: Tracking Fields: Destination Host Name

Event Count: 1 Span: 0 hrs 1 mins 0 secs Table Size: 100

Figure 5. Security Information Manager – User Access Monitor

Key Features and Benefits

Policy Manager

Defines and manages written policies

- Includes regulation and mandate content for Sarbanes-Oxley, PCI DSS, FISMA, HIPAA, GLBA, Basel II, and NERC
- Includes framework content for ISO 17799, COBIT (v3 and v4), and NIST SP800-53
- Sample policies and policy templates provide a starting point for strong IT compliance
- Easy to use policy creation wizard
- Policy risk rating

Distribute policies and track acceptance

- Target dissemination of policies to specific end-user groups
- Log all acceptance information for reporting and audit purposes
- Ensure that exceptions are reviewed and approved by appropriate policy owners and tagged with an expiration date
- Enhanced reports and dashboards capabilities

Map policies to regulations or frameworks to ensure and demonstrate coverage

- Report on compliance posture to multiple mandates
- Uniquely demonstrate compliance to policy by collecting evidence from procedural and technical data sources
- Mapping interface allows for ease of integration
- Enhanced integration with exception management and asset systems

Collect and display evidence for control objectives

- Provide best practice guidelines that translate vague regulatory requirements to actionable policy and collected evidence
- Perform risk-based analysis via an Impact Index (incorporating Confidentiality, Integrity, and Availability attributes to collected evidence)
- Map evidence directly to control statements, improving traceability between evidence and frameworks/regulations

Entitlement Manager

- Gather effective permission
  - Multiplatform support for Windows®, UNIX, Linux®, and Novell®
  - Support for Oracle and SQL Server databases
  - Automated discovery of control points based on files/directories/groups
- Report on effective permissions
  - Translate permissions into consistent human-readable format
  - Entitlement change reporting capabilities
  - Search and find data privileges easily
- Provide workflow for effective entitlements management
  - Assign business owners to operational data
  - Route entitlements to data owners for review and approval
  - Support for second-level approval
  - Ensure periodic review and approval of entitlements
  - Define management classifications
  - Enable business owners to effectively engage with IT when changes are needed

Response Module Assessment

Questionnaire creation and distribution

- Assess, store, and report responses for procedural controls data
- Provides out-of-the-box content based on popular standards and frameworks: BS 7799, COBIT, COSO, CSC, C-TPAP, HIPAA, FAA, FERPA, FFIEC, FISMA, GLBA, ISO 14001, ISO 27001, ISO 27799, ISO 20858, ITIL , MDA, OHSAS 18001, ONR 17700, PCI, NERC, NIST, and SOX
- Provides the ability to quickly create custom questionnaires
- Allows for multi-path (branching) assessment questions
- Supports many response types, including radio button, freeform, check boxes
- Associates surveys to respondents and assets
- Attach evidence to survey responses
- Deploys and scales easily using Web-based services
- Integration with CCS Asset system

Consolidated reporting of response

- Saves incomplete questionnaires and permits out-of-order response entry
- Allows for risk-based weighting of both questions and responses
- Provides end-user quizzing and certification
- Sets threshold values and retries
- Scores responses

Standards Manager

Create or select technical standards

- Broad, heterogeneous platform support allows for enterprise-wide coverage (see table in Technical Specifications)
- Supplies regulatory content for Sarbanes-Oxley, FISMA, HIPAA, GLBA, and Basel II, and framework content for ISO 17799, COBIT, and NIST SP800-53
- Includes best practices checks based on Center for Internet Security Standards (CIS), National Security Agency (NSA) benchmarks, and data from Symantec security experts

Assess controls

- Agentless technology eases deployment and maintenance
- Agent based technology supporting special platforms, i.e. AS/400, Sybase, MySQL
- Schedules jobs to reduce the cost of redundant and often-repeated technical assessments
- Integrated internet scanner provides a vulnerability assessment view
- Dashboard tool creates customizable reporting views of compliance posture

Detect deviations

- Reports pass/fail scores against standards to provide a view of security and compliance
- Manages exceptions to technical checks, thus ensuring appropriate review and approval, and automatically accounting for exceptions in reports
- Enhanced check-builder capabilities allow for better control
- Change auditing

Remediate deficiencies

- Ticketing system integration works within the existing organizational change control process

Security Information Manager

- Compliance and audit reporting
- Log retention and retrieval
- Real-time threat analysis
- Automated incident prioritization
- Incident remediation workflow
- Align security and compliance requirements with IT operations
- Meet compliance reporting requirements quickly and effectively
- Gain accurate and timely visibility into your security risk posture
- Increase IT staff productivity by prioritizing the most critical of security issues
- Reduce IT security operational costs and improve response time
- Provide appropriate security service levels to different business units and geographies

Fully Integrated and Automated

Risk Based

Flexible Deployment

New / Enhancement to CCS 9.0 Infrastructure

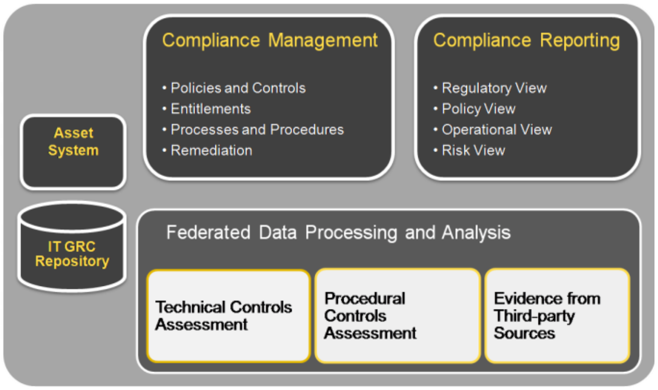
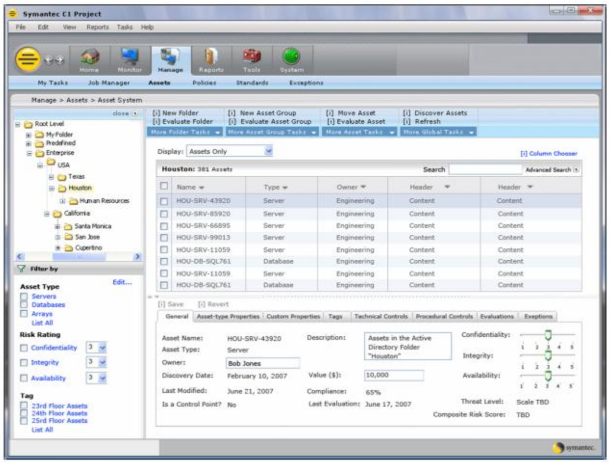


Figure 8. Control Compliance Function overview

Asset System

Scheduled, automated import of asset information from Asset management systems, CMDBs, etc. With the new Asset System and data repository, companies can now take an Asset-Centric approach to compliance and risk management. Through the automated reconciliation capabilities customers will always have the most up-to-date information available about an asset.

- ○ Centralized asset store with multiple predefined types
- ○ Site - New concept for associating assets to enterprise location
- ○ Using CSV data collector for custom asset types
- ○ Automated reconciliation and manual review
- ○ UI views of compliance measurement, risk scores, evidence, etc…



Asset Type
□ Servers
□ Databases
□ Arrays
List All

Risk Rating
□ Confidentiality 3
□ Integrity 3
□ Availability 3

Tag
□ 23rd Floor Assets
□ 24th Floor Assets
□ 25rd Floor Assets
List All

Display: Assets Only

Houston: 381 Assets

□	Name	Type	Owner	Header	Header
□	HOU-SRV-43920	Server	Engineering	Content	Content
□	HOU-SRV-85920	Server	Engineering	Content	Content
□	HOU-SRV-66895	Server	Engineering	Content	Content
□	HOU-SRV-99013	Server	Engineering	Content	Content
□	HOU-SRV-11059	Server	Engineering	Content	Content
□	HOU-DB-SQL761	Database	Engineering	Content	Content
□	HOU-SRV-11059	Server	Engineering	Content	Content
□	HOU-DB-SQL761	Database	Engineering	Content	Content

Asset Name: HOU-SRV-43920
Asset Type: Server
Owner: Bob Jones
Discovery Date: February 10, 2007
Last Modified: June 21, 2007
Is a Control Point? No
Description: Assets in the Active Directory Folder "Houston"
Value ($): 10,000
Compliance: 65%
Last Evaluation: June 17, 2007
Confidentiality: 3
Integrity: 3
Availability: 3
Threat Level: Scale TBD
Composite Risk Score: TBD

Figure 7. Assess Management UI

Risk Scoring

CCS allows customers to take a risk-based approach to managing compliance. In CCS 9.0 we've added Risk Scoring capability that allows a variety of risk based scoring based on standards, i.e. CIA values and others. The scoring formula is based on an industry standard CVSS (Common Vulnerability Scoring System) methodology

- Assess overall risk posture based on:
  - ○ Risk metrics assigned to checks and assets
  - ○ Scoring formula based on CVSS methodology
  - ○ Check metrics: (based on vulnerability/exploit potential)
  - ○ Asset metrics (based on asset importance)

Enhanced Compliance Reporting

- Dedicated report and dashboard processing subsystem
- Extensive list of predefined reports and dashboards
- Ability to distribute reports as e-mail attachments
- Support for Historical Data Management

Enhanced Exception Management

- Centralized exception management
- Exception templates to address application specific issues
- Role-based workflow for segregation of duties
- Notification sent on state change and prior to expiration

Enhancements to CCS applications

- Policy Management - New policy creation wizard, new mapping interface, enhanced integration, exception management, asset system, policy risk rating, enhanced reports and dashboards.
- Standards Management - Standards-based data collection, composite standards, enhanced check-builder, change auditing, extended platform support.
- Entitlements Management-Entitlement management for databases (Oracle and SQL Server), entitlement change reporting, enhanced reporting, exception management support for second-level approval.
- Response Assessment - Associate surveys to respondents and assets, attach evidence to survey response, integration with CCS Asset system quizzing, set threshold values, retries, score responses
- Security Information Manager 4.6 is now part of the CCS family. - Service Provider Architecture Support, Asset Grouping, Hierarchical Incident Creation, HoneyNet Intelligence Tab

More information

Visit our Web site
http://enterprise.symantec.com

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 Web site.

About Symantec
Symantec is a global leader in providing security, storage, and systems management solutions to help businesses and consumers secure and manage their information. Headquartered in Cupertino, California.

Symantec has operations in more than 40 countries.

More information is available at www.symantec.com.

Symantec World Headquarters
20330 Stevens Creek Blvd.
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com