



Compliance with the Payment Card Industry Data Security Standard

Meeting the Challenge
with Symantec Technology

Compliance with the Payment Card Industry Data Security Standard

Meeting the Challenge with Symantec Technology

Contents

Introduction	4
PCI Data Security Standard overview	5
PCI compliance challenges	7
PCI requirement 1: Install and maintain a firewall configuration to protect data	7
PCI requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	7
PCI requirement 3: Protect stored data	9
PCI requirement 4: Encrypt transmission of cardholder and sensitive information across public networks	9
PCI requirement 5: Use and regularly update antivirus software or programs	10
PCI requirement 6: Develop and maintain secure systems and applications	11
PCI requirement 7: Restrict access to data by business need-to-know	12
PCI requirement 8: Assign a unique ID to each person with computer access	13
PCI requirement 9: Restrict physical access to cardholder data (not covered by Symantec solutions)	14
PCI requirement 10: Track and monitor all access to network resources and cardholder data ..	15
PCI requirement 11: Regularly test security systems and processes	16
PCI requirement 12: Maintain a policy that addresses information security for employees and contractors	17

Compliance with the Payment Card Industry Data Security Standard Meeting the Challenge with Symantec Technology

Introduction

In 1999, Visa USA developed the Cardholder Information Security Program (CISP). The goal of this program was to assure cardholders that their account information was safe, regardless of where it was offered for payment. Originally intended to secure credit card transactions over the Internet, the CISP was expanded and mandated in June 2001 to apply to all payment channels, including retail (brick and mortar), mail/telephone order, and e-commerce.

To achieve CISP compliance, merchants and service providers must adhere to the Payment Card Industry (PCI) Data Security Standard. The PCI standard, the result of a collaboration between Visa and MasterCard, is designed to create common industry security requirements that incorporate the CISP requirements. Currently, the CISP and PCI Data Security Standard have been endorsed by Visa, MasterCard, American Express, Diner's Club, Discover, and JCB USA.

If a member, merchant, or service provider does not comply with the security requirements or fails to rectify a security issue, they may face fines of up to US\$500,000 per incident or restrictions imposed by the credit card companies, including denying their ability to accept or process credit card transactions. The final deadline for compliance with the PCI Data Security Standard was June 30, 2005.

Compliance with the Payment Card Industry Data Security Standard Meeting the Challenge with Symantec Technology

PCI Data Security Standard overview

The PCI Data Security Standard comprises 12 major requirements, supported by a set of detailed subrequirements. These security requirements apply to all system components, which are defined as any network component, server, or application included in, or connected to, the cardholder data environment. Network components include but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Servers include but are not limited to Web, database, authentication, Domain Name Service (DNS), mail, proxy, and Network Time Protocol (NTP). Applications include all purchased and custom applications, including internal and external Web applications.

Following are the 12 major requirements of the PCI Data Security Standard:

1. Install and maintain a firewall to protect data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.
3. Protect stored data.
4. Encrypt transmission of cardholder data and sensitive information across public networks.
5. Use and regularly update antivirus software.
6. Develop and maintain secure systems and applications (includes installing the latest security patches).
7. Restrict access to data by business need-to-know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security.

At a high level, these requirements seem fairly easy to implement and maintain. Upon closer examination, however, it becomes clear that attaining and maintaining compliance is a much more complex endeavor. This paper breaks down each requirement and details how Symantec solutions can help you get—and stay—compliant. It documents how Symantec products and solutions can address the sections of the PCI Data Security Standard listed in the following table. Only the sections and subsections that can be addressed using Symantec products and solutions are covered.

Compliance with the Payment Card Industry Data Security Standard Meeting the Challenge with Symantec Technology

PCI Requirement Description	Symantec Coverage
Requirement 1	Install and maintain a firewall configuration to protect data
Requirement 2 (2.1-2.2)	Do not use vendor-supplied defaults for system passwords and other security parameters
Requirement 3	Protect stored data
Requirement 4 (4.1)	Encrypt transmission of cardholder data and sensitive information across public networks
Requirement 5 (5.1-5.2)	Use and regularly update antivirus software
Requirement 6 (6.1-6.2)	Develop and maintain secure systems and applications
Requirement 7 (7.1-7.2)	Restrict access to data by business need-to-know
Requirement 8 (8.1, 8.4-8.5)	Assign a unique ID to each person with computer access
Requirement 9	Restrict physical access to cardholder data
Requirement 10 (10.1-10.5,10.7)	Track and monitor all access to network resources and cardholder data
Requirement 11 (11.2)	Regularly test security systems and processes.
Requirement 12	Maintain a policy that addresses information security for employees and contractors.

Symantec coverage of PCI requirements

Compliance with the Payment Card Industry Data Security Standard Meeting the Challenge with Symantec Technology

PCI compliance challenges

Symantec can assist organizations in complying with the PCI Data Security Standard. This section covers each requirement that our products and solutions address.

PCI requirement 1: Install and maintain a firewall configuration to protect data

This requirement mandates that basic perimeter security be used within the enterprise.

The problem: Organizations, by and large, have implemented firewalls at the perimeter. What they lack is an ability to decipher the enormous stream of firewall log data that is being generated to understand when critical exposures are occurring.

Symantec solutions: Symantec does not sell firewall equipment or software but does offer the technology to help ensure that firewall configurations are appropriate and to analyze firewall activity. Symantec™ Security Information Manager can consolidate information from disparate firewalls, logs, and other security monitoring devices, like intrusion detection systems and event logs, to determine the root cause of security failures and trigger remediation response, in real time.

PCI requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

This requirement is based on the fact that one of the simplest ways for internal or external intruders to compromise your systems is by using vendor default passwords and settings. These passwords and settings are generally publicly available.

Subsection 2.1

Always change the vendor-supplied defaults before you install a system on the network (for example, change passwords and SNMP community strings and eliminate unnecessary accounts).

The problem: This requirement mandates that companies have a set of standards for secure system builds, which must be verified prior to implementing the system on the network. In addition, the systems must be maintained after they have been installed, and manual tracking can be problematic.

Symantec solutions: Symantec™ Control Compliance Suite allows you to generate a thorough configuration report on a machine (server or workstation) prior to putting it into production. This report can be compared with your company's internal standards for secure server builds.

Compliance with the Payment Card Industry Data Security Standard Meeting the Challenge with Symantec Technology

Symantec also provides industry best practices for building and maintaining secure servers and applications.

After the system has been installed, Symantec can monitor it to help ensure that it stays in compliance with corporate or industry standards. We provide this functionality for both servers and workstations without requiring an agent on the target machines. In addition, by leveraging the integration between our solutions and enterprise monitoring tools such as HP OpenView® or Microsoft® Operations Manager, alerts can be generated and machines remediated to assure continued compliance.

Subsection 2.2

Develop configuration standards for all system components. Make sure these standards address all known security vulnerabilities and industry best practices. This subsection includes the following subrequirements:

- 2.2.1: Implement only one primary function per server (for example, Web servers, database servers, DNS, etc.).
- 2.2.2: Disable all unnecessary and insecure services and protocols.
- 2.2.3: Configure system security parameters to prevent misuse.
- 2.2.4: Remove all unnecessary functionality, such as scripts, drivers, subsystems, and file systems.

The problem: Keeping track of all the machines in an enterprise, down to the service and subsystem level, is a tedious task, especially in a large environment. It is even more difficult to monitor services, parameters, or protocols, for example, that would render a system prone to misuse. Even with good documentation and change management practices, ensuring that these systems meet this requirement is a tough challenge. The requirement also mandates that IT departments address all vulnerabilities and meet industry best practices. Staying on top of vulnerabilities and best practices can be a full-time job.

There are two ways to address this problem. The first is to manually configure each server so that it is secure, which is labor- and time-intensive. The second is to use an automated audit tool that allows every machine in the environment to be continuously monitored for compliance.

Compliance with the Payment Card Industry Data Security Standard Meeting the Challenge with Symantec Technology

Symantec solutions: Symantec Control Compliance Suite can ease the burden of documenting and monitoring your computing environment. It gathers information down to the service/daemon level to identify exactly what is running on each machine. This simplifies the task of making sure each server performs only a single function. Symantec vulnerability management tools are constantly and automatically updated to identify the latest threats and vulnerabilities in all computing environments. Additionally, Symantec Control Compliance Suite includes reports that are based on industry best practices for building secure servers (that is, Center for Internet Security Levels 1 and 2), so it is easy to stay up to date on maintaining a secure computing environment.

PCI requirement 3: Protect stored data

Data at rest requires protection from data extrusion, whether from external malware or internal misappropriation.

The problem: Critical data resides everywhere within the organization. For compliance with PCI requirements, credit card transaction information, which spans numerous application and server data stores, must be protected.

The solution: Symantec AntiVirus™ is an industry-leading solution for thwarting malware exploits. It provides protection against malicious intrusions, which are increasingly involving data theft. In addition, the Symantec Database Audit Security solution monitors transaction activity against databases and uses behavioral detection to sniff out and provide alerts on anomalous behavior. These solutions help protect against the increasing threat of data extrusion.

PCI requirement 4: Encrypt transmission of cardholder and sensitive information across public networks

The interception and diversion of data while it is in transit is a clear and present danger to the security of cardholder data. The best way to secure this sensitive information is to encrypt it prior to transmission over the Internet.

Subsection 4.1

Use strong cryptography and encryption techniques (of at least 128-bit), such as Secure Sockets Layer (SSL), PPTP, or IPSEC, to safeguard cardholder data during transmission over public networks.

Compliance with the Payment Card Industry Data Security Standard Meeting the Challenge with Symantec Technology

The problem: It is very important to make sure that all Web servers that even have a remote chance of handling cardholder data are utilizing encryption. Getting a handle on which servers are running Web services and how they are configured, however, is a time-consuming and labor-intensive manual process.

Symantec solutions: Symantec Control Compliance Suite allows organizations to quickly identify all Web servers in their computing environment and verify that they have SSL (128-bit) implemented.

PCI requirement 5: Use and regularly update antivirus software or programs

Worms, viruses, and spyware pose a major threat to the security of every organization. These malicious programs most commonly enter the network via end-user email activities and Web browsing. It is vital that all systems (servers and workstations) that are connected to the network are running antivirus software with the latest virus definition files installed.

Subsection 5.1

Deploy antivirus mechanisms on all systems commonly affected by viruses (for example, PCs and servers).

Subsection 5.2

Ensure that all antivirus mechanisms are current, actively running, and capable of generating audit logs.

The problem: Deploying antivirus software is not enough. Companies must also make sure that the antivirus software is up to date and actively running on every machine. This task is next to impossible to perform manually, especially in large environments.

Symantec solutions: Symantec provides a market-leading solution for enterprise antivirus to provide comprehensive coverage of this PCI requirement. Symantec solutions can also help organizations quickly and accurately ascertain which machines have antivirus software installed. More important, they can determine which virus definition files are being used and whether the antivirus software is actively running.

Compliance with the Payment Card Industry Data Security Standard Meeting the Challenge with Symantec Technology

PCI requirement 6: Develop and maintain secure systems and applications

Employees, external hackers, viruses, and worms can exploit security vulnerabilities to obtain privileged access to systems. Installing vendor security patches can protect many vulnerabilities from exploitation. All systems should have the most current security patches installed to maintain a secure computing environment.

Subsection 6.1

Ensure that all system components and software have the latest vendor-supplied security patches. Subsection 6.1.1 requires that all relevant security patches be installed within one month of release.

Subsection 6.2

Establish a process to identify newly discovered security vulnerabilities (that is, subscribe to alert services freely available on the Internet). Update your standards to address new vulnerability issues.

The problem: Keeping track of the latest security vulnerabilities on all platforms and applications installed in a computing environment is a challenge. Making sure that these security patches are then deployed across all systems (servers and workstations) and applications can be a logistical nightmare. The tight time constraints imposed by this requirement necessitate the use of an automated solution to track and deploy security patches.

Symantec solutions: Symantec Control Compliance Suite enables organizations to set up a customized profile for tracking vulnerabilities. Depending on the platforms and applications present in the enterprise environment, the solution can provide notifications that are filtered based on their profile.

Symantec has partnered with Shavlik Technologies to provide a world class patch management and deployment solution. This solution can monitor patch revision levels on every machine in an environment without the need for an agent. Additionally, Symantec can leverage this architecture to deploy patches in a fast, efficient manner. The solution helps to ensure that your systems (workstations and servers) and applications (Microsoft Office and other applications) are running with the most recent security patches.

Compliance with the Payment Card Industry Data Security Standard Meeting the Challenge with Symantec Technology

PCI requirement 7: Restrict access to data by business need-to-know

Restricting access to critical, confidential data on a need-to-know basis ensures that only authorized personnel can gain access to it. This restriction reduces the number of users with access to cardholder data, decreasing the risk of malicious use of this data.

Subsection 7.1

Limit access to computing resources and cardholder information to only those individuals whose job requires such access.

Subsection 7.2

Establish a mechanism for systems with multiple users that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed.

The problem: Identifying and controlling data access permissions across an enterprise is a daunting task. Tracking these controls manually, especially considering all aspects of the Microsoft security model, is tedious and labor-intensive, even with native tools and utilities. Calculating permissions manually and/or taking shortcuts when attempting to define effective entitlements can lead to false positives or negatives. The process is so complex that most enterprises simply accept the risk of not documenting data access controls, making them noncompliant with this standard.

Symantec solutions: Symantec Control Compliance Suite can calculate file access permissions in large distributed environments. Symantec has addressed every aspect of the Microsoft security model. File share and NTFS permissions (both directly assigned and inherited), effective group membership (including nested groups), effective local and network access rights, and effective user privileges (Backup, Restore, Take Ownership) are all taken into account when calculating total effective permissions.

This solution can determine what a user has access to, what a group has access to, or what objects have rights to access specific data. Additionally, it can illustrate exactly how these rights were calculated. To help ensure that access is given only according to a business need-to-know, the solution has a Web-based interface that can track access permissions by data owner/business unit and allow data owners to sign off on this access.

Compliance with the Payment Card Industry Data Security Standard Meeting the Challenge with Symantec Technology

Symantec Control Compliance Suite can also report on user access rights and permissions on both the Oracle® and Microsoft SQL Server platforms. Database security is another crucial area in the fight to maintain secure cardholder information.

PCI requirement 8: Assign a unique ID to each person with computer access

Assigning a unique ID to every individual helps ensure that actions taken on critical data and systems can be traced to known and authorized users.

Subsection 8.1

Identify all users with a unique user name before allowing them to access system components or cardholder data.

Subsection 8.4

Encrypt all passwords during transmission and storage on all system components.

Subsection 8.5

Ensure proper user authentication and password management for nonconsumer users and administrators on all system components. This section includes the following subrequirements:

- 8.5.1: Control the addition, deletion, and modification of user IDs, credentials, and other identifier objects.
- 8.5.2: Verify user identity before performing password resets.
- 8.5.3: Set first-time passwords to a unique value per user and change immediately after first use.
- 8.5.4: Immediately revoke accesses of terminated users.
- 8.5.5: Remove inactive user accounts at least every 90 days.
- 8.5.6: Enable accounts used by vendors for remote maintenance only during the time needed.
- 8.5.7: Distribute password procedures and policies to all users who have access to cardholder information.
- 8.5.8: Do not use group, shared, or generic accounts/passwords.
- 8.5.9: Change user passwords at least every 90 days.
- 8.5.10: Require a minimum password length of at least seven characters.
- 8.5.11: Use passwords containing both numeric and alphabetic characters.
- 8.5.12: Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.

Compliance with the Payment Card Industry Data Security Standard Meeting the Challenge with Symantec Technology

- 8.5.13: Limit repeated access attempts by locking out the user ID after not more than six attempts.
- 8.5.14: Set the lockout duration to 30 minutes or until the administrator enables the user ID.
- 8.5.15: If a session has been idle for more than 15 minutes, require the user to reenter the password to reactivate the terminal.
- 8.5.16: Authenticate all access to any database containing cardholder information.
This includes access by applications, administrators, and all other users.

The problem: The main areas addressed by this requirement are user and password management. Both are problematic because without a set of tools to automate the associated tasks, they are delegated to skilled personnel (usually help desk administrators). Additionally, it is vital to monitor domain password policies for any changes that may affect compliance with this requirement. In combination, the tasks involved with meeting this requirement can incur significant labor cost.

Symantec solutions: Symantec does not offer identity management solutions for user provisioning. Symantec Control Compliance Suite, however, provides the ability to determine and report on adherence to user provisioning policies, for example, whether stale accounts are being deleted, password policies are being adhered to, and so on. As a result, Symantec works in conjunction with identity management solutions to help ensure that appropriate identity administration activities are taking place.

PCI requirement 9: Restrict physical access to cardholder data (not covered by Symantec solutions)

Compliance with the Payment Card Industry Data Security Standard Meeting the Challenge with Symantec Technology

PCI requirement 10: Track and monitor all access to network resources and cardholder data

Logging mechanisms and the ability to track user activities are critical for forensic analysis in the event of a problem. Determining the cause or extent of a compromise is next to impossible without a thorough set of system activity logs.

Subsection 10.1

Establish a process for linking all access to system components (especially those with administrative privileges such as root) by an individual user.

Subsection 10.2

Implement automated audit trails to reconstruct the following events for all system components:

- 10.2.1: All individual user accesses to cardholder data
- 10.2.2: All actions taken by any individual with root or administrative privileges
- 10.2.3: Access to all audit trails
- 10.2.4: Invalid logical access attempts
- 10.2.5: Use of identification and authentication mechanisms
- 10.2.6: Initialization of the audit logs
- 10.2.7: Creation and deletion of system-level objects

Subsection 10.3

Record at least the following audit trail entries for each event, for all system components:

- 10.3.1: User identification
- 10.3.2: Type of event
- 10.3.3: Date and time
- 10.3.4: Success or failure indication
- 10.3.5: Origination of event
- 10.3.6: Identity or name of affected data, system component, or resource

Subsection 10.4

Synchronize all critical system clocks and times.

Compliance with the Payment Card Industry Data Security Standard Meeting the Challenge with Symantec Technology

Subsection 10.5

Secure audit trails so they cannot be altered, including the following subset (which Symantec can address):

- 10.5.1: Limit viewing of audit trails to those with a job-related need.
- 10.5.2: Protect audit trail files from unauthorized modifications.
- 10.5.3: Promptly back up audit trail files to a centralized log server or media that is difficult to alter.

Subsection 10.6

Retain your audit trail history for a period that is consistent with its effective use, as well as legal regulations. (An audit history usually covers a period of at least one year, with a minimum of three months available online.)

The problem: This requirement creates two related tasks. The first is to make sure that auditing is set up throughout the environment on all systems. This in itself is a highly labor-intensive process, since it requires the manual review of all audit settings on all machines in an environment.

Once auditing has been enabled, it must be consolidated, reviewed, secured, and archived for a defined time period. Without an automated tool, this second task is also difficult and labor-intensive.

Symantec solutions: Symantec Security Information Manager can consolidate audit logs from over 100 different applications and cross-correlate events to conduct root cause analysis, alert in real time for security breaches, and enable a remediation response workflow to manage incident response.

PCI requirement 11: Regularly test security systems and processes

Managing vulnerabilities as they are identified and introduced into an environment is a challenging task. For this reason, it is important that systems, processes, and custom software be tested frequently to ensure that security is maintained over time and through changes.

Subsection 11.2

Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (that is, new system component installations, changes in network topology, firewall rule modifications, product upgrades). External vulnerability scans must be performed by a scan vendor qualified by the payment card industry.

Compliance with the Payment Card Industry Data Security Standard Meeting the Challenge with Symantec Technology

The problem: It is critical to scan your network for vulnerabilities on a regular basis. While external vulnerability scans must be performed by an outside vendor, using such a vendor to perform regular internal vulnerability scans can become prohibitively expensive.

Symantec solutions: Symantec Control Compliance Suite provides a platform-independent IP scanning tool. Any device connected to the network can be scanned for vulnerabilities on a scheduled or ad hoc basis. This is more than a simple port scanner. It scans for a multitude of vulnerabilities and threats using methods similar to those a hacker might employ. The checks that are packaged with this solution are updated on a regular basis, making it easy to stay on top of the latest threats and vulnerabilities.

Since all external vulnerability scans must be performed by a qualified vendor, Symantec solutions are limited to internal vulnerability scans of the network. This is still a vital part of maintaining a secure computing environment. Note that many external vendors use Symantec solutions for vulnerability scanning.

PCI requirement 12: Maintain a policy that addresses information security for employees and contractors

A strong security policy is essential for letting employees know what is expected of them. They should all be acutely aware of the sensitivity of cardholder information and know their responsibilities for protecting this information.

Subsection 12.1

Establish, publish, maintain and disseminate a security policy that:

- 12.1.1: Addresses all requirements in this specification
- 12.1.2: Includes an annual process that identifies threats and vulnerabilities and that results in a formal risk assessment
- 12.1.3: Includes a review at least once a year and is updated when the environment changes

Subsection 12.2

Develop daily operational security procedures that are consistent with the requirements in this specification (that is, user account maintenance procedures and log review procedures).

Compliance with the Payment Card Industry Data Security Standard Meeting the Challenge with Symantec Technology

Subsection 12.3

Develop usage policies for critical employee-facing technologies, such as modems and wireless, to define the proper use of these technologies for all employees and contractors. Ensure that these usage policies require:

- 12.3.1: Explicit management approval.
- 12.3.2: Authentication for use of the technology.
- 12.3.3: A list of all such devices and personnel with access.
- 12.3.4: Labeling of devices with owner, contact information, and purpose.
- 12.3.5: Acceptable uses of the technology.
- 12.3.6: Acceptable network locations for these technologies.
- 12.3.7: A list of company-approved products.
- 12.3.8: Automatic disconnect of modem sessions after a specific period of inactivity.
- 12.3.9: Activation of modems for vendors only when needed by vendors, with immediate deactivation after use.
- 12.3.10: When accessing cardholder data remotely via modem, disable storage of cardholder data onto local hard drives, floppy disks, or other external media. Also, disable cut-and-paste and print functions during remote access.

Subsection 12.4

Ensure that security policies and procedures clearly define information security responsibilities for all employees and contractors.

Subsection 12.6

Make all employees aware of the importance of cardholder information security:

- 12.6.1: Educate employees (for example, through posters, letters, memos, meetings, and promotions).
- 12.6.2: Require employees to acknowledge in writing that they have read and understood the company's security policy and procedures.

Compliance with the Payment Card Industry Data Security Standard Meeting the Challenge with Symantec Technology

Subsection 12.9

Implement an incident response plan. Be prepared to respond immediately to a systems breach.

This section includes the following subrequirements:

- 12.9.1: Create an incident response plan to be used in the event of system compromise. Ensure that the plan addresses, at a minimum, specific incident response procedures, business recovery and continuity procedures, data backup processes, roles and responsibilities, and communication and contact strategies (for example, informing acquirers and credit card associations).
- 12.9.2: Test the plan at least annually.
- 12.9.3: Designate specific personnel to be available 24 hours a day, seven days a week to respond to alerts.
- 12.9.4: Provide appropriate training to staff with security breach response responsibilities.
- 12.9.5: Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems.
- 12.9.6: Have a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.

The problem: This requirement creates several tasks that Symantec can address. It involves the creation and publication of security policies and procedures that cover the responsibilities of employees and contractors. It also requires that these policies and procedures be reviewed and accepted in writing. Finally, it requires the creation and testing of an incident response plan. These policies, procedures, and plans require in-depth knowledge of security and technology.

Symantec solutions: Symantec Control Compliance Suite's Policy Module solution assists with the creation, dissemination, and user acceptance tracking of security policies and procedures. This tool includes templates and best practices and the ability to securely store policies in an easy-to-use, Web-based format. It also can track user acceptance of these policies, proving that employees and contactors have read, understood, and accepted their responsibilities as they pertain to securing cardholder data.

About Symantec

Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world.

The company helps customers protect their infrastructure, information, and interactions by delivering software and services that address risks to security, availability, compliance, and performance. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries.

More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

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

Copyright © 2006 Symantec Corporation. All rights reserved. Symantec, the Symantec logo, and Symantec AntiVirus are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners. Printed in the U.S.A.
12/06 10705119