The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version: 6.0

Legal Notice

Copyright © 2011 Symantec Corporation. All rights reserved.

Symantec and the Symantec Logo 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.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1
Getting Started

This document includes the following topics:

- About Symantec Protection for SharePoint Servers
- What's new
- Components of Symantec Protection for SharePoint Servers
- Before you install
- About deployment options (stand-alone and farm environments)
- Upgrading to version 6.0
- System requirements
- About installing Symantec Protection for SharePoint Servers
- About the installation options
- Post-installation tasks
- Where to get more information

About Symantec Protection for SharePoint Servers

Symantec™ Protection for SharePoint® Servers provides virus scanning and repair services for the following SharePoint products:

- Windows® SharePoint® Services 2.0 (WSS 2.0)
- Windows SharePoint Services 3.0 (WSS 3.0)
- Microsoft Office SharePoint® Server 2007 (MOSS 2007)
In addition to virus scanning and repair services, Symantec Protection for SharePoint Servers provides logging, monitoring, and reporting of infected documents on the SharePoint server.

What's new

Table 1-1 describes the new features in Symantec Protection for SharePoint Servers.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enhanced User Interface</td>
<td>Symantec Protection for SharePoint Servers now has an enhanced User Interface.</td>
</tr>
<tr>
<td>Quarantine Management</td>
<td>You can manage all the quarantined files from a single location. Based on your requirements, you can either restore or delete the quarantined files.</td>
</tr>
<tr>
<td>Import/Export Settings</td>
<td>You can import Symantec Protection for SharePoint Servers settings from one SharePoint deployment to another SharePoint deployment when you have multiple SharePoint deployments on your network.</td>
</tr>
<tr>
<td>Integration with the latest Symantec Scan Engine 5.2</td>
<td>Symantec Protection for SharePoint Servers has the latest version of Symantec Scan Engine 5.2 for virus scanning and repair services. Symantec Scan Engine 5.2 includes new features like support for up to 80 scan engines, Rapid Release update of definitions and so on. For more information, see the Symantec Scan Engine Implementation Guide.</td>
</tr>
</tbody>
</table>

Components of Symantec Protection for SharePoint Servers

Symantec Protection for SharePoint Servers includes the following components, which you can install and configure separately:
Symantec Scan Engine: Provides virus scanning and repair services. You can install Symantec Scan Engine on the SharePoint server. You can also install Symantec Scan Engine on a separate server that is not running SharePoint. This lets you move antivirus processing off-box, thereby reducing the CPU load on the SharePoint server. The latest version of Symantec Scan Engine 5.2 is included in the software package.

Symantec Protection for SharePoint console: Provides a means for users to configure how Symantec Scan Engine and the SharePoint server should communicate with each other, handle infected files, and monitor scanning activity. The Symantec Protection for SharePoint console refers to the administrative console of Symantec Protection for SharePoint Servers. You can configure how Symantec Protection for SharePoint Servers handles the communication between the Symantec Scan Engine and the SharePoint server through this console. Symantec Protection for SharePoint Servers also interprets the results that are returned from the scan engine after scanning.

Before you install

Do the following tasks before you install Symantec Protection for SharePoint Servers or its components:

- Provide antivirus protection for the servers on which the Symantec Protection for SharePoint Servers components run.
- Exclude certain directories from scanning by any other antivirus product that is running on the computers on which you install the components.

To prevent a conflict between the antivirus product that is running on the host computer and Symantec Protection for SharePoint Servers, configure any other antivirus product that is running on the host computer to exclude certain directories from scanning.

Table 1-2 lists the directories to exclude from scanning.
Table 1-2  Directories to exclude from scanning

<table>
<thead>
<tr>
<th>Directories</th>
<th>Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows:&lt;Installdir&gt;\temp</td>
<td>The server on which Symantec Scan Engine runs.</td>
</tr>
<tr>
<td>Linux® and Solaris™:&lt;Installdir&gt;/temp</td>
<td>These directories are the temporary directories that Symantec Scan Engine uses for scanning.</td>
</tr>
<tr>
<td>&lt;Installdir&gt;\Program Files\Symantec SharePoint\Quarantine</td>
<td>The server on which Symantec Protection for SharePoint console runs.</td>
</tr>
<tr>
<td></td>
<td>This is the default quarantine directory that is used by Symantec Protection for SharePoint Servers.</td>
</tr>
</tbody>
</table>

- Plan to install the Symantec Protection for SharePoint console at a time when Microsoft Internet Information Server (IIS) can be stopped temporarily. Microsoft IIS restarts automatically after the installation is complete.

- Ensure that the computer on which you plan to install the console and Symantec Scan Engine meets the minimum system requirements. You can install both components together or on separate computers.

- Ensure that the ports 9455, 9466 and 9477 are available.

- For a SharePoint 2003/2007 stand-alone deployment, ensure that SharePoint is not configured with Microsoft SQL Server Desktop Engine or Windows Internal Database.
  Symantec Protection 6.0 for SharePoint Servers does not support a SharePoint stand-alone configuration with Microsoft SQL Server Desktop Engine or Windows Internal Database.

- Symantec recommends that you back up the web.config file of the SharePoint Central Administration site.

### About deployment options (stand-alone and farm environments)

You must install Symantec Protection for SharePoint Servers differently based on whether you have a stand-alone SharePoint environment or a farm environment. For a stand-alone environment, you can choose the option of a full install of both components of Symantec Protection for SharePoint Servers on the same server. You can also install the Symantec Protection for SharePoint console...
and Symantec Scan Engine on separate computers. However, ensure that you install the Symantec Protection for SharePoint console on the SharePoint server.

For more information on accessing the Central Administration console, see the *Symantec Protection for SharePoint Servers Implementation Guide*.

In a SharePoint farm environment, based on the SharePoint version, install the Symantec Protection for SharePoint console on the following servers:

**WSS 2.0/SPS 2003**
- Install the Symantec Protection for SharePoint console on each front-end web server in the farm.
- Symantec Scan Engine, the other component, can be installed on the same server as the Symantec Protection for SharePoint console or on a separate server.

**WSS 3.0/MOSS 2007**
- Install the Symantec Protection for SharePoint console on each front-end web server in the farm and at least on one server where Central Administration service is running.
- You can install the Symantec Protection for SharePoint console on the other Application servers in the farm to run on-demand or scheduled scans on these servers, if desired. However, you can run these scans from the front-end servers as well.
- Symantec Scan Engine, the other component, can be installed on the same server as the Symantec Protection for SharePoint console or on a separate server.

**Microsoft SharePoint Foundation 2010/Microsoft Office SharePoint Server 2010**
- Install the Symantec Protection for SharePoint console on each front-end Web server in the farm and at least on one server where Central Administration service is running.
- You can install the Symantec Protection for SharePoint console on the other Application servers in the farm to run on-demand or scheduled scans on these servers, if desired. However, you can run these scans from the front-end servers as well.
- You can install Symantec Scan Engine on the same server as the Symantec Protection for SharePoint console or on a separate server.

---

### Upgrading to version 6.0

Symantec Protection for SharePoint Servers supports an upgrade from older versions of the product. The installation program does one of the following when it detects a previous version of Symantec Protection for SharePoint Servers:
Symantec AntiVirus for Microsoft SharePoint (version 4.3): The installation program does not detect Symantec AntiVirus for Microsoft SharePoint (version 4.3). You must manually uninstall it before you install Symantec Protection 6.0 for SharePoint Servers.

Symantec Protection for SharePoint Servers (version 5.1.x): If the installation program detects an older version of Symantec Protection for SharePoint Servers, it uninstalls Symantec Protection for SharePoint Servers version 5.1.x and then installs Symantec Protection 6.0 for SharePoint Servers. The installation program does not retain any settings from the older version of the product.

System requirements

You can choose to install both components of Symantec Protection for SharePoint Servers together on the same computer or on different computers. The Symantec Protection for SharePoint console and Symantec Scan Engine are supported on both 32-bit and 64-bit computers for Windows 2003 Server and Windows 2008 Server.

See “System requirements for Symantec Protection for SharePoint Servers integrated installation” on page 8.

See “System requirements for Symantec Protection for SharePoint console only” on page 9.

See “System requirements for Symantec Scan Engine” on page 11.

System requirements for Symantec Protection for SharePoint Servers integrated installation

Table 1-3 describes the minimum system requirements to install the Symantec Protection for SharePoint console and Symantec Scan Engine on the same server.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware requirements</td>
<td>■ Processor and Memory: As per the requirements of the version of Microsoft SharePoint</td>
</tr>
<tr>
<td></td>
<td>■ Disk space: 515 MB</td>
</tr>
<tr>
<td></td>
<td>■ 1 network interface card (NIC) running TCP/IP with a static IP address</td>
</tr>
<tr>
<td></td>
<td>■ Internet connection to update antivirus definitions</td>
</tr>
</tbody>
</table>
Table 1-3 Minimum system requirements for Symantec Protection for SharePoint console and Symantec Scan Engine (continued)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Symantec Protection for SharePoint Servers runs on the following platforms:</td>
</tr>
<tr>
<td></td>
<td>■ Windows Server 2003 (32-bit and 64-bit) with Service Pack 2 or later</td>
</tr>
<tr>
<td></td>
<td>■ Windows Server 2008 (32-bit and 64-bit) with Service Pack 2 or later</td>
</tr>
<tr>
<td></td>
<td>You can use any of the following editions of Windows Server:</td>
</tr>
<tr>
<td></td>
<td>■ Windows Server 2003 Standard/Enterprise/Data Center SP2/R2</td>
</tr>
<tr>
<td></td>
<td>■ Windows Server 2008 Standard/Enterprise/Data Center SP2/R2</td>
</tr>
<tr>
<td>Software requirements</td>
<td>Any of the following Microsoft SharePoint Server editions:</td>
</tr>
<tr>
<td></td>
<td>■ Windows SharePoint Services 2.0 (WSS 2.0) with Service Pack 3 (SP 3)</td>
</tr>
<tr>
<td></td>
<td>■ SharePoint Portal Server 2003 (SPS 2003) with Service Pack 3 (SP 3)</td>
</tr>
<tr>
<td></td>
<td>■ Windows SharePoint Services 3.0 (WSS 3.0)</td>
</tr>
<tr>
<td></td>
<td>■ Microsoft Office SharePoint Server 2007</td>
</tr>
<tr>
<td></td>
<td>■ Microsoft SharePoint Foundation 2010</td>
</tr>
<tr>
<td></td>
<td>■ Microsoft Office SharePoint Server 2010</td>
</tr>
<tr>
<td></td>
<td>Any of the following Web browsers:</td>
</tr>
<tr>
<td></td>
<td>■ Microsoft Internet Explorer® 6.0 or higher (for Microsoft SharePoint 2003/2007)</td>
</tr>
<tr>
<td></td>
<td>■ Microsoft Internet Explorer® 7.0 or higher (for Microsoft SharePoint 2010)</td>
</tr>
<tr>
<td></td>
<td>The following software components:</td>
</tr>
<tr>
<td></td>
<td>■ Microsoft .NET Framework 2.0 SP1 or higher</td>
</tr>
<tr>
<td></td>
<td>■ Microsoft ASP.NET 2.0 AJAX Extensions 1.0 (only for Microsoft SharePoint 2003/2007)</td>
</tr>
<tr>
<td></td>
<td>■ Central Admin Site ASP.NET Version 2.0 or higher</td>
</tr>
</tbody>
</table>

System requirements for Symantec Protection for SharePoint console only

Table 1-4 describes the minimum system requirements to install the Symantec Protection for SharePoint console.
### Table 1-4 Minimum system requirements for the Symantec Protection for SharePoint console

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Details</th>
</tr>
</thead>
</table>
| Hardware requirements | ■ Processor and Memory: As per the requirements of the version of Microsoft SharePoint  
■ Disk space: 50 MB (may vary depending on how long you choose to maintain log files) |
| Operating System | Symantec Protection for SharePoint Servers runs on the following platforms:  
■ Windows Server 2003 (32-bit and 64-bit) with Service Pack 2 or later  
■ Windows Server 2008 (32-bit and 64-bit) with Service Pack 2 or later  
You can use any of the following editions of Windows Server:  
■ Windows Server 2003 Standard/Enterprise/Data Center SP2/R2  
■ Windows Server 2008 Standard/Enterprise/Data Center SP2/R2 |
| Software requirements | Any of the following Microsoft SharePoint Server editions:  
■ Windows SharePoint Services 2.0 (WSS 2.0) with Service Pack 3 (SP 3)  
■ SharePoint Portal Server 2003 (SPS 2003) with Service Pack 3 (SP 3)  
■ Windows SharePoint Services 3.0 (WSS 3.0)  
■ Microsoft Office SharePoint Server 2007  
■ Microsoft SharePoint Foundation 2010  
■ Microsoft Office SharePoint Server 2010  
Any of the following Web browsers:  
■ Microsoft Internet Explorer® 6.0 or higher (for Microsoft SharePoint 2003/2007)  
■ Microsoft Internet Explorer® 7.0 or higher (for Microsoft SharePoint 2010)  
The following software components:  
■ Microsoft .NET Framework 2.0 SP1 or higher  
■ Microsoft ASP.NET 2.0 AJAX Extensions 1.0 (only for Microsoft SharePoint 2003/2007)  
■ Central Admin Site ASP.NET Version 2.0 or higher |
System requirements for Symantec Scan Engine

You can install Symantec Scan Engine on Windows, Linux, and Solaris.

See “Windows system requirements” on page 11.

See “Solaris system requirements” on page 12.

See “Linux system requirements” on page 13.

Windows system requirements

The following are the system requirements to install Symantec Scan Engine on Windows:

Operating system
- Windows 2000 Server with the latest service pack
- Windows Server 2003 (32-bit and 64-bit)
- Windows Server 2003 R2 (32-bit and 64-bit)
- Windows Server 2008 (32-bit and 64-bit)
- Windows Server 2008 R2 (32-bit and 64-bit)

Processor
Pentium 4 processor 1 GHz or higher

Memory
1 GB of RAM or higher

Disk space
500 MB

Hardware
- 1 network interface card (NIC) running TCP/IP with a static IP address
- Internet connection to update definitions
- 100 Mbit/s Ethernet link (1 Gbit/s recommended)
Software
- J2SE Runtime Environment (JRE) 5.0 (update 13 or later) or JRE 6.0
  The most current version of JRE 5.0 and JRE 6.0 at the time of product ship is provided in the software package in the following folder: Java\Win32
- Any of the following Web browsers:
  - Microsoft Internet Explorer 6.0 (with the most recent service pack that is available)
    Use Microsoft Internet Explorer to access the Symantec Scan Engine console from a Windows client computer.
  - Mozilla Firefox® 1.5 or later
    Use Mozilla Firefox to access the Symantec Scan Engine console from a Solaris or Linux client computer.

The Web browser is only required for Web-based administration. The Web browser must be installed on a computer from which you want to access the Symantec Scan Engine console. The computer must have access to the server on which Symantec Scan Engine runs.

Solaris system requirements
The following are the system requirements to install Symantec Scan Engine on Solaris:

- **Operating system**  
  Solaris 9 and 10
  Ensure that your operating system has the latest patches that are available.

- **Processor**  
  SPARC®

- **Memory**  
  1 GB of RAM or higher

- **Disk space**  
  500 MB

- **Hardware**
  - 1 network interface card (NIC) running TCP/IP with a static IP address
  - Internet connection to update definitions
  - 100 Mbit/s Ethernet link (1 Gbit/s recommended)
Software

- J2SE Runtime Environment (JRE) 5.0 (update 13 or later) or JRE 6.0
  The most current version of JRE 5.0 and JRE 6.0 at the time of product ship is provided in the software package in the following folder: Java\Solaris
  If you install the self-extracting JRE, ensure that you note the installation location. You must provide the location of the JRE if the installer is unable to detect it.
- Any of the following Web browsers:
  - Microsoft Internet Explorer 6.0 (with the most recent service pack that is available)
    Use Microsoft Internet Explorer to access the Symantec Scan Engine console from a Windows client computer.
  - Mozilla Firefox 1.5 or later
    Use Mozilla Firefox to access the Symantec Scan Engine console from a Solaris or Linux client computer.

The Web browser is only required for Web-based administration. The Web browser must be installed on a computer from which you want to access the Symantec Scan Engine console. The computer must have access to the server on which Symantec Scan Engine runs.

Linux system requirements

The following are the system requirements to install Symantec Scan Engine on Linux:

Operating system

- Red Hat® Linux Enterprise Server 3 and 4
- Red Hat Linux Advanced Server 3 and 4
- Red Hat Enterprise Linux 5
- SUSE Linux® Enterprise Server 9 and 10
- Red Hat Enterprise Linux 5 (64-bit)

Processor

Pentium 4 processor 1 GHZ or higher

Memory

1 GB of RAM or higher

Disk space

500 MB

Hardware

- 1 network interface card (NIC) running TCP/IP with a static IP address
- Internet connection to update definitions
- 100 Mbit/s Ethernet link (1 Gbit/s recommended)
Software

- Ensure that the following packages are installed:
  - GNU sharutils-4.6.1-2 or later
    Use this package to expand the Rapid Release packages.
  - ncompress-4.2.4-44 or later
    Use this package to expand the Rapid Release packages.
  - GNU C Library (glibc)
  - initscripts
    This package is required for Red Hat Linux only.
  - aaa_base package
    This package is required for SUSE only.
  - J2SE Runtime Environment (JRE) 5.0 (update 13 or later) or JRE 6.0
    The most current version of JRE 5.0 and JRE 6.0 at the time of product ship is provided in the software package in the following folder: Java\RedHat
    Install the JRE using Red Hat Package Manager (RPM). Ensure that you note the installation location. You must provide the location of the JRE if the installer is unable to detect it.
  - Any of the following Web browsers:
    - Microsoft Internet Explorer 6.0 (with the most recent service pack that is available)
      Use Microsoft Internet Explorer to access the Symantec Scan Engine console from a Windows client computer.
    - Mozilla Firefox 1.5 or later
      Use Mozilla Firefox to access the Symantec Scan Engine console from a Solaris or Linux client computer.

The Web browser is only required for Web-based administration. The Web browser must be installed on a computer from which you want to access the Symantec Scan Engine console. The computer must have access to the server on which Symantec Scan Engine runs.

**About installing Symantec Protection for SharePoint Servers**

Symantec Protection for SharePoint Servers comprises the following components:

- Symantec Scan Engine
- Symantec Protection for SharePoint console

Based on the SharePoint farm environment and SharePoint version used, install the Symantec Protection for SharePoint console on all servers in the farm or only on the Application server.
During installation, Symantec Protection for SharePoint Servers installs both components together or separately based on the installation option that you choose.

The Symantec Protection for SharePoint Servers installation program checks for previous versions of the product and does one of the following:

No previous version is detected

Based on the installation option you choose, the installation program performs a full installation of Symantec Protection for SharePoint Servers and its components.

A previous version of either component is detected

The installation program does one of the following when it detects a previous version of Symantec Protection for SharePoint Servers or any of its components:

- Symantec AntiVirus for Microsoft SharePoint (version 4.3): The installation program does not detect Symantec AntiVirus for Microsoft SharePoint (version 4.3). You must manually uninstall it before you install Symantec Protection 6.0 for SharePoint Servers.

- Symantec Protection for SharePoint Servers (version 5.1.x): If the installation program detects an older version of Symantec Protection for SharePoint Servers, it uninstalls Symantec Protection for SharePoint Servers version 5.1.x and then installs Symantec Protection 6.0 for SharePoint Servers. The installation program does not retain any settings from the older version of the product.

- Symantec Scan Engine 5.1x: If the installer detects Symantec Scan Engine 5.1x, it upgrades Symantec Scan Engine 5.1x to 5.2x.

- Symantec Scan Engine 4.3: If the installer detects Symantec Scan Engine 4.3, you are not allowed to proceed with the installation unless you uninstall the previous version.

During installation of Symantec Scan Engine, you can enter the file path of a valid license for automatic license activation. Symantec Protection for SharePoint Servers automatically registers the Symantec Scan Engine if you enter the license file path during a full installation. When you register Symantec Scan Engine during the installation process, you eliminate the need to register it through the Symantec Protection for SharePoint console.

If you install Symantec Scan Engine separately, you can still enter the license file path during installation. Automatic activation occurs if the license is valid.
However, you must register Symantec Scan Engine manually with Symantec Protection for SharePoint Servers.

Symantec Scan Engine installs a virtual administrative account during installation. Do not forget the password for this account because it is the only account that you can use to manage Symantec Scan Engine. You can change the password in the console, but to do so you must have the old password.

If you do not have the license file at the time of installation, you can activate the license later through the Symantec Scan Engine console.

The installation program installs the Symantec Protection for SharePoint console using the service logon details that you enter during the installation procedure. You can change the service logon details after installation. You can also password protect the console so that unauthenticated users cannot access or modify the settings.

You can use the silent installation or remote installation feature for multiple installations on your network.

For more information about how to perform silent upgrades or installation, see the Symantec Protection for SharePoint Servers Implementation Guide.

About the installation options

On a Windows platform, the software installer displays the following options:

- Install Symantec Protection 6.0 for SharePoint Servers (Full Install)
  - Installs both Symantec Scan Engine and the Symantec Protection for SharePoint console.

- Install only the Symantec Scan Engine 5.2
  - Installs Symantec Scan Engine only.

- Install only the Symantec Protection for SharePoint console
  - Installs the administrative console for Symantec Protection for SharePoint Servers

On a Linux/Solaris platform, you can install Symantec Scan Engine only. This is because only Symantec Scan Engine is supported on Linux or Solaris.

Post-installation tasks

The post-installation tasks are as follows:
Access the Symantec Protection for SharePoint console

Enable real-time scanning

Install the license for Symantec Scan Engine
   This step is required if you did not install the license during installation.

Register the Symantec Scan Engine with the Symantec Protection for SharePoint console

Configure Symantec Scan Engine

Enable security risk detection

Configure Symantec Protection for SharePoint Servers

For more information, see the *Symantec Protection for SharePoint Servers Implementation Guide*.

Where to get more information

In addition to this guide, Symantec Protection for SharePoint Servers includes Help topics that you can access through the Help table of contents and index. You can also search for keywords in the Help.

Context-sensitive help is available on each page.

You can visit the Symantec Web site for more information about your product.

The following online resources for Symantec Protection for SharePoint Servers are available:

- Provides access to the technical support Knowledge Base, news groups, contact information, downloads, and mailing list subscriptions

- Provides product news and updates

- Provides access to the Virus Encyclopedia, which contains information about all known threats; information about hoaxes; and access to white papers about threats
Where to get more information