

Symantec AntiVirus™ Corporate Edition 10.2

Automated defense and response against the latest viruses, spyware, and adware, now supporting Windows Vista™

Availability	2
What is Symantec AntiVirus Corporate Edition?	2
Value Statements	2
Target Market.....	3
Key Points.....	4
What's New?.....	5
Continuing Features & Benefits.....	5
System Requirements.....	12
Services, Support and Maintenance.....	13

Control Information

Date First Issued	November 30, 2006
Date Last Revised	October 26, 2006
Audience	Symantec global sales
Distribution Control	Limited initially to Symantec employees. After legal review, channel partner and customer versions will be available.
Author	Claudia Malaspina-Slane, Sales Tools and Proposals

Availability

Following are the first customer ship dates in each region (subject to change without notice). Consult your regional marketing manager for launch dates and activities.

Region	Language	First Customer Ship
North America	English	November 30, 2006
LAM	List all available languages	TBD based on localization
EMEA	List all available languages	TBD based on localization
APAC	List all available languages	TBD based on localization
Japan	List all available languages	TBD based on localization

What is Symantec AntiVirus Corporate Edition?

Symantec AntiVirus™ Corporate Edition combines industry-leading, real-time malware protection for enterprise workstations and network servers with graphical Web-based reporting, centralized management and administration capabilities. Side-effect repair keeps systems operational during security disruptions. Centralized configuration and deployment eases administrative burden and overhead. Integrated response content helps maximize system uptime.

Value Statements

Customer Need	Simplicity	Automation	Virus/spyware Protection
Value Proposition	Symantec AntiVirus provides automatic defense and response against viruses and spyware/adware throughout the enterprise.		
How We Deliver	Ease of administration and scalability.	Responsive intelligence and control.	Threat detection, removal and repair.
Key Messages	<ul style="list-style-type: none"> Enables administrators to manage client and server groups by creating and deploying security policies. Configure automatic updates for virus definitions and push updates to keep systems compliant. Comprehensive view of client via centralized logging, threshold alerting, and 	<ul style="list-style-type: none"> Minimize administrator involvement with automatic detection and repair capabilities. Behavior blocking prevents client systems from being used for malicious outbound activities. Optimize response time and reduce network bandwidth through 	<ul style="list-style-type: none"> Advanced repair capability automatically detects and repairs viruses, spyware, and effects of other malicious intrusions. Inoculate and quarantine a fast-spreading threat in your environment by initiating an on-demand LiveUpdate session (where LiveUpdate is a

	<p>graphical reporting helps transform security data into actionable information.</p> <ul style="list-style-type: none"> • Deploy bug fixes, security fixes and upgrade new versions at minimal cost, time and risk using methods compatible with existing Symantec AntiVirus investment. • Highly scalable for extensive use throughout even the largest enterprise. 	<p>incremental virus definitions deployed to client machines and network servers.</p> <ul style="list-style-type: none"> • Automatically identify connected workstations and network servers that do not have Symantec AntiVirus protection installed to help ensure highest level of protection. • Global intelligence and worldwide response team provides extensive coverage and support to equip your administrators with knowledge of the latest threats. 	<p>scheduled event).</p> <ul style="list-style-type: none"> • Help protect confidential information in files, processes and registry entries from unauthorized access and attacks.
--	---	--	---

Target Market

This release will continue the strategy of targeting Big Spenders, Risk Averse Controllers, and Security Bulldogs as the primary focus and Minimalists and Mainstream Basics as secondary targets. Enhanced reporting capabilities should facilitate our success across organizations of all sizes.

	Big Spenders	Risk Averse Controllers	Security Bulldogs	Mainstream Basics	Minimalists
Overall Spend	44%	24%	23%	8%	1%
SCM Spend	34%	44%	6%	10%	6%
Ability to Execute	<ul style="list-style-type: none"> ▶40% of current business ▶2nd largest qty of non-customers 	<ul style="list-style-type: none"> ▶35% of current business ▶1st largest qty of non-customers 	<ul style="list-style-type: none"> ▶8% of current business 	<ul style="list-style-type: none"> ▶13% of current business 	<ul style="list-style-type: none"> ▶8% of current business
How to reach	Field/SIs	VAR/Reseller	Field/SIs	Field	Retailer
Organizational Size Breakdown within Segment	Large 55% Medium 40% Small 5%	Large 10% Medium 42% Small 48%	Large 4% Medium 30% Small 66%	Large 24% Medium 57% Small 19%	Large 6% Medium 36% Small 58%
What to build	<ul style="list-style-type: none"> ▶High quality reporting ▶Enables Compliance ▶Scalable ▶Integrated solution 	<ul style="list-style-type: none"> ▶Interoperable ▶Prevents threats/breaches ▶Cares less about integration 	<ul style="list-style-type: none"> ▶Prevents threats/breaches ▶Easy to maintain ▶Interoperable ▶Easy to deploy 	<ul style="list-style-type: none"> ▶Prevents threats/breaches ▶Good Service 	<ul style="list-style-type: none"> ▶Good value for the money

Key Points

- Advanced, enterprise-wide virus protection and monitoring from a single management console
- NEW! Microsoft® Windows Vista client support
- Integrated Web-based graphical reporting
 - Scales to support thousands of users
 - Simple installation
 - Streamlined workflow and usability
 - Available reports meet primary administrative needs
- Effective protection from spyware and adware, including:
 - Spyware repair enhancements automatically block spyware installation
 - Stealthed spyware detection and remediation
 - View spyware impact based on Symantec's Risk Impact Matrix
 - Spyware repairs for invasive risks
- Symantec tamper protection guards against unauthorized antivirus access and attacks, protecting users from viruses that attempt to disable security measures
- Backed by Symantec Security Response, the world's leading Internet security research and support organization

What's New

Feature	Description	Benefits
New	Microsoft Windows Vista Support	Delivers continuous virus and spyware protection – helping to ensure that all workstations on the new Vista OS are protected from today's rapidly evolving malware attacks.

Continuing Features & Benefits

Feature	Description	Benefits
Real-time Detection of Spyware and Adware	<p>Symantec AntiVirus Corporate Edition 10.2 uses the real-time scanning capabilities of Symantec's antivirus technology to detect spyware that attempts to run or install on a machine. On detection the spyware will be removed from the machine.</p> <p>Ease of Management</p> <p>The addition of spyware /adware functionality will not require any infrastructure changes or added cost for customers. Simplified and familiar management capabilities allow even the smallest organization to achieve enterprise-scale protection and control.</p> <p>Exclusions</p> <p>Exclusions provide administrators the flexibility to set their own security policies for spyware and adware. Administrators can decide on an application-by-application basis whether to allow or block spyware, which allows companies to designate certain applications as acceptable for their organizations.</p> <p>Automatic Removal</p> <p>Symantec AntiVirus Corporate Edition 10.2 now provides automated repair of the side effects from today's blended threats, spyware and adware. When blended threats, spyware or adware are detected, repair is automatically triggered to reverse the changes made to users' systems</p>	<ul style="list-style-type: none"> Helps detect and prevent spyware from spreading throughout the company infrastructure.



Feature	Description	Benefits
	<p>with no need for administrator intervention.</p> <p>Side Effect Repair</p> <p>Whereas viruses can often be removed by the deletion of a single file, spyware makes changes to users' files, registry entries and system load points, making clean up and removal a difficult task. Symantec AntiVirus Corporate Edition 10.0 automates that removal, launches repair when spyware is detected, and helps restore systems to a spyware-free state.</p>	
<p>Product Security</p> <p>Easy, Centralized Management for Up-to-Date Protection</p>	<p>Tamper Protection product security technology protects against attacks to Symantec AntiVirus Corporate Edition 10.2 from malicious code writers.</p> <p>Enterprise-wide Protection from a Single Console</p> <p>Offers a proven management infrastructure, the Symantec System Center, to make it easy for administrators to install, configure, and update Symantec AntiVirus Corporate Edition from a central location, across a variety of desktop and server platforms.</p> <p>Easy Installation and Deployment</p> <p>Offers flexible, easy installation and deployment of all or selected components by using the new MSI installer. Administrators can either:</p> <p>Deploy the solution immediately by selecting from three; pre-configured installation packages (managed client, lightly managed client, and thin client).</p> <p>Design custom deployment packages to fit their organizational needs.</p> <p>Logical Group Management</p> <p>Enables administrators to create logical groups of like workstations and servers so they can:</p> <ul style="list-style-type: none"> • Manage multiple functional groups from a single parent server. • Apply policy settings quickly and easily as appropriate to each group 	<ul style="list-style-type: none"> • Helps protect product from unauthorized access and attacks • Saves the time and cost of traveling from machine to machine. • Helps to ensure that servers and desktops stay updated and properly configured. • Makes deployment easier, saving administrator time/effort and lowering costs. • Provides greater flexibility through its modular design to meet the unique needs of varying environments. • Eases manageability • Improves scalability. • Minimizes the number of servers needed to manage diverse groups of clients and servers.

Feature	Description	Benefits
	<p>Network Audit</p> <p>Includes centralized network auditing capabilities that enable administrators to identify:</p> <ul style="list-style-type: none"> • Which workstations and network servers do not have antivirus protection installed. • Which workstations and network servers are protected by Symantec AntiVirus Corporate Edition and select third-party antivirus products. <p>Centralized Logging and Alerting</p> <p>Alerts administrators immediately to virus activity within their network via several methods:</p> <ul style="list-style-type: none"> • Pager • Internet e-mail • Message box • SNMP trap notices • Network broadcast alerts to domains, systems, or users <p>Also, provides complete, centralized event logging, which administrators can easily view, query, and sort.</p> <p>Threat Tracer</p> <p>Enables administrators to identify which machine has generated a threat that is spreading by an open file share (for example, Nimda or CodeRed).</p> <p>VPN Compliancy Check – Symantec VPN Sentry— Performs the following compliancy checks for Symantec clients after establishing a VPN tunnel but before granting VPN access to the corporate network:</p> <ul style="list-style-type: none"> • Is Symantec AntiVirus installed? • Is real time protection (Auto-Protect) enabled? • Is Auto-Protect heuristic virus scanning enabled at the specified level? • Is Auto-Protect configured to scan on specified types of file access? • Did a LiveUpdate™ session complete successfully within a specified number of days? • Is the installed Symantec antivirus client at least a specified minimum version? • Are virus definitions files no older than a specified maximum age? • Has a specified scan run within the last (n) days? • Are the Microsoft® Exchange and/or Microsoft Outlook® plug-in scanner installed and enabled? • Is the Lotus Notes® plug-in scanner installed and enabled. 	<ul style="list-style-type: none"> • Reduces the risk of virus infiltration/infection by enabling administrators to proactively secure their workstations and network servers from virus attack • Helps to ensure system uptime and prevent data/productivity loss. • Helps increase system uptime and IT credibility by enabling administrators to pinpoint and eliminate virus threats quickly and completely. • Matches the right level of security to specific systems. • Identifies the source of an attack. • Helps ensure that clients have appropriate security before connecting to corporate network resources. • Reduces the threat of an outsider infecting the corporate infrastructure.

Feature	Description	Benefits
<p>Scalability</p>	<p>“Drag-and-Drop” Clients</p> <p>Enables administrators to easily move clients (who have changed departments, for example) from one physical parent server to another simply by dragging and dropping through the central management console.</p> <p>Store and Forward Event Data</p> <p>Stores event data generated while a client is disconnected from the corporate network and forwards it when the client reconnects.</p> <p>Enforceable LiveUpdate™</p> <p>Enables administrators to launch an immediate LiveUpdate session on single or multiple clients during an outbreak. A current maintenance contract is required in order to receive protection updates via LiveUpdate. One year of Gold Maintenance is bundled with Symantec AntiVirus Corporate Edition.</p> <p>Easy Support Access</p> <p>Offers a live link to Symantec’s support website directly from the Symantec System Center console.</p> <p>Easy Migration</p> <p>Overlays older versions of Symantec’s desktop and server antivirus software automatically during the installation process.</p> <p>Uses a tiered architecture with primary and secondary server support that enables administrators to configure Symantec AntiVirus Corporate Edition to automatically redirect client systems to secondary servers if a primary server fails—eliminating the possibility of a single point of failure. <i>Supports up to 180,000 clients per parent server.</i></p>	<ul style="list-style-type: none"> • Saves administrator time. • Minimizes the cost associated with managing diverse groups of users. • Helps ensure that potentially threatening event data is not overlooked. • Helps administrators better monitor and manage their mobile PCs. • Helps minimize response time to fast spreading threats. • Provides instant access to Symantec Enterprise Support for the latest information on viruses, Symantec’s Knowledge Base, and more. • Eliminates the need to leave the Symantec System Center console to access service and support information. • Saves time and helps reduce total cost of ownership. • Symantec has tested Symantec AntiVirus Corporate Edition to perform at a high client-to-server ratio, with negligible degradation in performance. • Symantec AntiVirus Corporate Edition can grow with an organization.

Feature	Description	Benefits
Rapid Virus Resolution	<p>Reduces the turnaround time on new virus submissions and cures by using the following intelligent, back-end services and exclusive response mechanisms.</p> <ul style="list-style-type: none"> • Cross-Platform Engine Updates—Updates the antivirus scanning and repair engine, using extensible engine technology, to protect against new virus classes that traditional virus definitions alone cannot address. The engine updates are automatically applied as customers download their new virus definitions—without stopping real-time scanning or re-starting servers. Enables administrators to rapidly deploy the same set of virus definitions across all machines, platforms, and network tiers. • Quarantine Server—Centralizes virus management by enabling administrators to redirect un-repairable, virus-infected files to a safe area on a centralized server for further inspection. • Automated Virus Submission/Response—Submits suspicious, quarantined files to Symantec Security Response via the Internet (HTTPS), without administrator intervention, then automatically returns the virus cure. Administrators can test the virus cure first or deploy it directly to the infected systems or the entire enterprise. • Back-end Automation—uses automated tools to analyze macro virus samples and to develop cures for them without human intervention at Symantec Security Response. • Quarantine Console—Enables administrators to centrally manage all activity in the Quarantine Server, allowing them to: <ul style="list-style-type: none"> • Visually track quarantined files. • Test virus fixes received from Symantec Security Response. • Automatically roll out virus fixes to infected client machines. • “Flood Control”—Helps avoid potential bottlenecks that could occur as customers submit virus-infected files to Symantec Security Response during widespread virus infections by automatically redirecting traffic from overwhelmed servers and adding additional servers before flood conditions arise. • Rapid Virus Cure Deployment—uses multithreading technology to deploy virus definition updates on multiple servers simultaneously. Administrators simply download an update from Symantec Security Response onto a primary server, and the update automatically cascades (pushes) to multiple secondary (parent) servers and client desktop/server machines. 	<ul style="list-style-type: none"> • Saves time and hassle; eliminates gaps in protection and helps lower cost of ownership • Provides greater protection by removing viruses from the main computing environment and preventing them from spreading inside the organization • Makes it easy to submit infected files; provides fast response, and eliminates reliance on e-mail—particularly critical when a virus has disabled the mail server • Makes response times even faster and helps get systems up-and-running faster • Provides up-to-the minute status and added control. • Helps ensure timely response to new virus outbreaks • Enables fast deployment of virus cures and, thus, faster response to security threats, which is crucial during a virus outbreak or security breach.

Feature	Description	Benefits
<p>Proven Virus Protection</p>	<p>Multi-Platform Support</p> <p>Provides continuous, unobtrusive protection against viruses, malicious code, and Trojan horses across a variety of mixed-desktop and server platforms, including:</p> <p>Workstations:</p> <ul style="list-style-type: none"> • Windows® 2000 Professional, Server, Advanced Server • Windows XP Home, Professional, Tablet PC, and 64-Bit • Windows Server 2003 Web, Standard, Enterprise, and Datacenter Editions • Windows Server 2003 Enterprise and Datacenter 64-Bit <p>Server:</p> <ul style="list-style-type: none"> • Windows 2000 Professional, Server, Advanced Server • Windows XP Professional • Windows Server 2003 Web, Standard, Enterprise, and Datacenter Editions. <p>Up-to-Date Protection with LiveUpdate*</p> <ul style="list-style-type: none"> • Enables administrators to download virus definition updates from Symantec Security Response via the Internet during installation and to schedule future, automatic updates to run as often as the organization's security policy requires. • Uses incremental technology to retrieve only the new virus definitions since the previous update, rather than all available virus definitions, reducing the virus definition file size from 4.2 megabytes to approximately 80K. <p>*A current maintenance contract is required in order to receive protection updates via LiveUpdate. One year of Gold Maintenance is bundled with Symantec AntiVirus Corporate Edition.</p> <p>Rapid, Reliable, Configurable Scanning</p> <ul style="list-style-type: none"> • Uses multithreading technology to scan multiple files simultaneously. • Scans cached files (files in memory), as well as files on the hard drive. • Enables end users to: <ul style="list-style-type: none"> • Delay an administrator-scheduled scan when they require maximum computing resources. • Adjust scan priority to scan during idle time only. • Scan their remote laptops only when connected to AC power 	<p>Provides the protection organizations need in today's heterogeneous environments.</p> <ul style="list-style-type: none"> • Eases the management burden of manually initiating the update process during outbreak situations. • Ensures that updates occur even during unexpected outbreak situations on weekends or evenings. • Speeds the update process and minimizes network traffic. • Enables administrators to respond to threats quicker and more proactively.

Feature	Description	Benefits															
	<p>Virus Detection and Repair in Compressed Files</p> <p>Detects and repairs viruses in compressed files automatically—including nested compressed files—ensuring that even well-hidden viruses do not enter a customer's network. Compressed file formats include:</p> <table data-bbox="512 678 1126 913"> <tr> <td>Zip[®]</td> <td>SYMC Ghost Image</td> <td>HTTP</td> </tr> <tr> <td>LZH/LHA</td> <td>Bin Hex</td> <td>MS Compressed</td> </tr> <tr> <td>Mime/UU</td> <td>TAR</td> <td>OLESS Containers</td> </tr> <tr> <td>Cab</td> <td>GNU</td> <td>MS-TNEF</td> </tr> <tr> <td>Arc Manager</td> <td>UUE</td> <td>Rich Text Format</td> </tr> </table> <p>Executable Files</p> <p>E-mail Attachment Scanning (Windows 2000 only)</p> <p>Automatically scans incoming Lotus Notes, Microsoft Exchange, and POP3 e-mail messages and attachments on client machines to prevent viruses from entering end user systems.</p> <p>Behavior Blocking—Outbound E-mail Worm Heuristics</p> <p>Detects applications that attempt to spawn themselves over the network or Internet by e-mail. This feature is of particular importance with the pervasiveness of mass-mailer worms that typically contain their own SMTP engine for self-propagation.</p> <p>Roaming Client Support</p> <ul data-bbox="534 1579 1145 1769" style="list-style-type: none"> • Provides built-in roaming client support, which enables end users who travel from site to site to retrieve virus definition updates from the closest and fastest parent server. • Recognizes when traveling users are disconnected from the network, delaying their scheduled LiveUpdate sessions until they have re-connected. 	Zip[®]	SYMC Ghost Image	HTTP	LZH/LHA	Bin Hex	MS Compressed	Mime/UU	TAR	OLESS Containers	Cab	GNU	MS-TNEF	Arc Manager	UUE	Rich Text Format	<ul data-bbox="1206 443 1525 1693" style="list-style-type: none"> • Provides greater protection and makes downloading files off the Internet safer. • Provides protection against fast-moving, e-mail-based threats. • Protects against propagation of worms that spread via e-mail, like SoBig. • Saves time and helps reduce online costs. • Helps ensure that end users' virus protection stays current even while they are traveling.
Zip[®]	SYMC Ghost Image	HTTP															
LZH/LHA	Bin Hex	MS Compressed															
Mime/UU	TAR	OLESS Containers															
Cab	GNU	MS-TNEF															
Arc Manager	UUE	Rich Text Format															

System Requirements

For full System Requirements, please refer to the [Data Sheet](#) on SCORE posted on SCORE

Symantec AntiVirus for 32-Bit and 64-Bit (Windows Vista)

Windows Vista

Minimum system requirements of the operating system required for Symantec AntiVirus clients running on Windows Vista

Symantec AntiVirus for 32-Bit (Non-Windows Vista)

Windows 2000 Professional/Server/Advanced Server; Windows XP Home/Professional/Tablet PC; Windows Server 2003 Web/Standard/Enterprise/Datacenter

64 MB RAM

55 MB disk space

Symantec AntiVirus for 640Bit Windows Clients (Non-Windows Vista)

Windows XP 64-Bit Edition Version 2003, Windows Server 2003 Standard/Enterprise/Datacenter 64-Bit Editions

80 MB RAM

70 MB disk space

Microsoft Internet Explorer 5.5 SP2 or later

Intel processors that support Intel Extended Memory 64 Technology (Intel EM64T)

AMD 64-Bit Opteron and Athlon processors

Note: Symantec AntiVirus Corporate Edition CD includes Symantec AntiVirus 10.1.x for Windows 2000, 2003, XP, and Netware; Symantec AntiVirus 10.2 for Vista; and Symantec AntiVirus 1.0.x for Linux.

Support and Maintenance

Enterprise Support at a Glance

Enterprise Support and Maintenance Services	Basic Maintenance	Essential Support	Business Critical Services*			
			Remote Product Specialist	DataCenter	National	Global
Severity One Response Time Targets	1 hour	30 minutes	15 minutes	15 minutes	15 minutes	15 minutes
Telephone Access to Support Engineers	8 a.m.-6 p.m. Business Hours,	24x7x365	24x7x365	24x7x365	24x7x365	24x7x365
Downloadable software upgrades, updates, and patches	♦	♦	♦	♦	♦	♦
Designated Callers	2 per Product Title	6 per Product Title	6 per Product	Unlimited	Unlimited	Unlimited
Remote Product Specialist			♦			
Business Critical Account Manager (BCAM)				Remote BCAM	Designated BCAM	Global BCAM
Business Critical Engineer				♦	♦	♦
Onsite Visits (Fly-to-Site)				2	6	20
Tailored Account Support Plan					♦	♦
Quarterly Account Reviews					♦	♦
Account Case History Reports					♦	♦
Network Link Assessment				Option	♦	♦
Impact Alerts					♦	♦

*See the [Business Critical Services General QuickStart](#) for additional features available only for BCS

Copyright © 2006 Symantec Corporation. All rights reserved. Symantec, the Symantec logo, Symantec AntiVirus, Symantec Brightmail AntiSpam, and LiveUpdate are trademarks or registered trademarks of Symantec Corporation or its affiliates in the United States and other countries. Other names may be trademarks of their respective owners.