



OVERVIEW

Symantec™ Multi-tier Protection safeguards enterprise assets and lowers risk by providing unmatched protection against threats for multiplatform network environments, mobile devices, mail servers and SMTP gateways.

Endpoint Protection: Symantec Multi-tier Protection includes the next-generation antivirus solution, Symantec™ Endpoint Protection, which combines Symantec AntiVirus™ with advanced threat prevention to deliver an unmatched defense against malware for laptops, desktops, and servers. It delivers the most advanced technology available to protect against today's sophisticated threats and threats not seen before. It includes proactive technologies that automatically analyze application behaviors and network communications to detect and actively block threats. It also provides device and application control features to manage actions and help secure data. This multi-layered approach significantly lowers risk and increases confidence that business assets are protected. Symantec Endpoint Protection is simple to implement and deploy. It integrates with Symantec's Altiris endpoint management solutions making it easier to distribute software packages, migrate older Symantec AntiVirus or other antivirus deployments and view deployment status and rollout activity. Symantec Multi-tier Protection also includes Symantec AntiVirus for Linux® (client only), Symantec AntiVirus for Macintosh®, and Symantec Mobile AntiVirus for Windows Mobile.

Groupware Protection: Symantec Mail Security for Microsoft Exchange and Symantec Mail Security for Domino provide highly effective email protection against viruses and threats while enforcing company security policies on Exchange and Domino servers. Symantec Premium AntiSpam™, based on the Symantec Brightmail™ antispam technology, offers 97% antispam effectiveness and less than one in a million false positive rate. It integrates seamlessly with Symantec Mail Security products to provide best-in-class antispam protection.

Gateway Protection: The Symantec™ Brightmail™ Gateway delivers effective and accurate antispam and antivirus protection for both inbound and outbound email and instant messaging (IM). It also features advanced content filtering and data loss prevention that helps organizations control sensitive data and meet regulatory compliance. Brightmail Gateway is simple to administer and catches more than 97% of spam with less than one in a million false positives. It is available in both a traditional physical appliance form factor, and a VMware-certified virtual appliance form factor, enabling customers to easily add or remove antispam capacity to keep messages flowing in the face of growing and unpredictable spam volume.

Note: Symantec Multi-tier Protection 11.0.2 is a product bundle and is not a single integrated product. The following Symantec products are tied together in a single package called Symantec Multi-tier Protection 11.0.2.

- Symantec Endpoint Protection – Advanced antivirus protection for Microsoft operating systems
- Symantec AntiVirus for Macintosh – Antivirus protection for MacOS
- Symantec AntiVirus for Linux – Antivirus protection for Linux clients
- Symantec AntiVirus for Windows Mobile – Antivirus protection for Windows® Mobile operating systems
- Symantec Mail Security for Domino – Antivirus for Domino server
- Symantec Mail Security for MS Exchange – Antivirus for MS Exchange server
- Symantec Premium AntiSpam protection for Domino server and MS Exchange server
- Symantec Brightmail Gateway Software Subscription and virtual appliance for SMTP gateway protection

Symantec Endpoint Protection Product Family

	SYMANTEC ENDPOINT PROTECTION	SYMANTEC MULTI-TIER PROTECTION SMALL BUSINESS EDITION	SYMANTEC MULTI-TIER PROTECTION
Antivirus	X	X	X
Antispyware	X	X	X
Desktop Firewall	X	X	X
Intrusion Prevention	X	X	X
Device and Application Control	X	X	X
Symantec Mail Security for Microsoft Exchange		X	X
Symantec Mail Security for Domino			X
Symantec AntiVirus for Macintosh		X*	X
Symantec AntiVirus for Linux	X	X	X



	SYMANTEC ENDPOINT PROTECTION	SYMANTEC MULTI-TIER PROTECTION SMALL BUSINESS EDITION	SYMANTEC MULTI-TIER PROTECTION
Symantec AntiVirus for Windows Mobile			X*
Symantec Premium AntiSpam		X*	X*
Symantec Brightmail Gateway Software Subscription			X*

Gray area = centrally managed via a single agent (Symantec Endpoint Protection Client) and single console (Symantec Endpoint Protection Manager)
 Note: Customers have the option to use the Symantec Brightmail Gateway software subscription on the hardware appliance (add-on); or deploy it as a virtual appliance. VM ware is not included.
 * New additions

VALUE PROPOSITION

For organizations that need a single, integrated solution to protect against sophisticated attacks that evade traditional security measures, Symantec Multi-tier Protection safeguards enterprise assets and lowers risk by providing unmatched protection against threats for laptops, desktops, mobile devices, mail servers, and SMTP gateways. It includes both endpoint and email protection to deliver superior protection against today's sophisticated threats.

Endpoint Protection

Symantec Multi-tier Protection includes the next-generation antivirus solution, Symantec Endpoint Protection, which combines Symantec AntiVirus™ with advanced threat prevention to deliver an unmatched defense against malware for laptops, desktops, and servers. It includes proactive technologies that automatically analyze application behaviors and network communications to detect and actively block threats. It also provides device and application control features to manage actions and secure data. Symantec Multi-tier Protection also includes Symantec AntiVirus for Windows® Mobile, Linux®, and Macintosh®, providing comprehensive virus protection against malicious threats that target Windows® Mobile operating systems, Linux and Macintosh systems.

Groupware Protection:

The Symantec Mail Security family protects and manages Microsoft Exchange and Domino servers against viruses, spam and security risks while enforcing compliance and HR policy by monitoring email and blocking offensive content. Symantec Premium AntiSpam™ provides multi-layered spam prevention which leverages multiple filtering technologies, including spam signatures, heuristics, reputation filters, language identification, and proprietary methods. The 99.9999% accuracy rate ensures that end-users do not miss any legitimate mail.

Gateway Protection:

Symantec Brightmail Gateway effectively and transparently responds to new spam threats to minimize network downtime, preserve employee productivity, and protect company reputation. Unlike products that are hard to use and force a choice between effectively catching spam and letting legitimate messages through, Brightmail Gateway is simple to administer and catches more than 97% of spam with less than one in a million false positives. Advanced content filtering and structured data protection support helps organizations control sensitive data, reduce the risks associated with data loss, and meet regulatory compliance and corporate governance demands. Powerful on-demand reporting, unified administrative controls, and flexible work flow simplify ongoing management and drive down administrative costs. Brightmail Gateway also offers different form factors to allow flexible deployment.

BUSINESS CHALLENGES

CUSTOMER PAIN POINTS	HOW WE DELIVER
Complex Endpoint Security Environments	<ul style="list-style-type: none"> Combines essential endpoint security technologies (Symantec Multi-tier Protection 11.0.2 includes Symantec Endpoint Protection 11.0) into a single agent Offers a single management console reducing administrative burden
Protect Data, Email and Windows and Non-window Devices from Growing Threats	<ul style="list-style-type: none"> Provides advanced threat prevention protecting from both known and unknown threats (through Symantec Endpoint Protection 11.0) Removes viruses from email attachments, Internet downloads, etc safeguarding the enterprise network.



CUSTOMER PAIN POINTS	HOW WE DELIVER
	<ul style="list-style-type: none"> Includes Symantec AntiVirus for Macintosh, Symantec AntiVirus for Windows Mobile, and Symantec AntiVirus for Linux
Reduce Costs Associated with Managing Multiple Endpoint Security Solutions	<ul style="list-style-type: none"> Symantec Endpoint Protection 11.0 reduces procurement, support and maintenance costs utilizing a single agent and single management console
Prove Internal and External Regulation / Compliance with Security Policies	<ul style="list-style-type: none"> Enforces company email security policies Enforces endpoint security policies (e.g., antivirus and firewall is on before being allowed to connect the corporate network)
Protect and Control of Spam for Emails and IM for the Messaging Infrastructure	<ul style="list-style-type: none"> Supports efforts to control spam related threats on the messaging (email and IM) infrastructure Messaging gateway security capabilities that blocks spam at the outer most layer
Filtering Message Content to Remove Unwanted Content and Protect IP from Data Leakage	<ul style="list-style-type: none"> Extremely flexible filtering technology coupled with checkbox-like ease of deployment makes implementing effective regulatory compliance and corporate governance easier

Additional Business Needs to Consider

- **Seamlessly integrated network access control** combines *Symantec Network Access Control* with Symantec™ Endpoint Protection, both of which utilize the same agents and management console to provide your organization with a seamless, necessary toolset.
- **Advanced protection for enterprise servers** specifically designed to protect servers such as file server, mail server, web servers etc. *Symantec Critical System Protection* combined with Symantec™ Endpoint Protection couples standard and advanced protection for heterogeneous server environments: UNIX, Linux and Solaris in addition to the Windows Server.
- **Protection for Smartphone and PDA's** by combining *Symantec Mobile Security Suite version 5.0 for Windows Mobile* with Symantec™ Endpoint Protection, which offers protection for Windows and non-Windows Mobile devices like Symbian and Palm OS.
- **Protection for data being accessed via unmanaged devices** using *Symantec On-Demand Protection*. Protects systems accessing web-enabled applications, such as web mail (MS Outlook Web Access), and the data moved onto unmanaged endpoints during the user sessions.
- **Data Loss Prevention on the Endpoint:** Symantec Endpoint Encryption 6.0 provides advanced encryption for desktops, laptops, and removable storage devices. It offers scalable, enterprise-wide security that prevents unauthorized access by using strong access control and powerful encryption.

PARTNER OPPORTUNITIES

PARTNER PAIN POINTS	HOW TO DELIVER
Improves Profitability	<ul style="list-style-type: none"> Partners up-selling Symantec Multi-tier Protection 11.0.2 with the Essential maintenance plan can increase their revenue while providing more support and satisfaction to their customers Leverages the new competitive cross-grade pricing to sell Symantec Multi-tier Protection 11.0.2 into competitive antivirus environments Channel partners have an opportunity to increase their revenue by selling 2-3 year maintenance contracts to new and existing customers coming up for renewal Partners moving customers from Express Buying programs to Rewards will see a drastic increase in their renewal rate which can represent incremental revenue annually Cross-sell Symantec Network Access Control to existing Symantec Client Security and Symantec AntiVirus once customers have migrated to Symantec Multi-tier Protection 11.0.2
Lack of Unified Security Solutions	<ul style="list-style-type: none"> Standardize security solutions for your customer base Expand your security services by recommending a platform solution Extend your expertise and reduce point vendor products carried

SELLING SERVICES

- Partner Services gives partners the opportunity to increase customer support by offering their own services around assessment, migration, implementation of Symantec Multi-tier Protection 11.0.2 and Symantec Network Access Control 11.0, as well as the entire Symantec Endpoint Security product line.

Professional Services – Remote Expert Installation Services	<ul style="list-style-type: none"> • Let Symantec install software for your customers and earn some more money! • Reduces the risks typically associated with upgrades and implementations • Improves the time-to-benefit of the software • Flexible, cost-effective knowledge transfer
Managed and Hosted Services – Education Services	<ul style="list-style-type: none"> • Best practice usage • Unrivaled product training expertise • Flexible, cost-effective knowledge transfer • Improves the business value of IT
Enterprise Support Services and Responses – Enterprise Support Services	<ul style="list-style-type: none"> • Maximizes availability • Flexible, cost-effective knowledge transfer • Industry-recognized support expertise • Flexible support plans

FOR MORE DETAILED INFORMATION AND QUOTING SAMPLES, PLEASE CONSULT THE LICENSING AND SUPPORT SERVICES GUIDE

KEY FEATURES AND BENEFITS

What's in Symantec Multi-tier Protection 11.0.2?

FEATURE	DESCRIPTION	BENEFIT
Multi-layered Protection	<ul style="list-style-type: none"> • Seamlessly integrates industry leading protection technologies (antivirus, antispysware, desktop firewall, IPS, and device control) in a single agent • Delivers both traditional-signature-based protection with behavioural-based proactive protection providing the ability to enable the pieces you need, as you need them 	<ul style="list-style-type: none"> • Gives comprehensive protection against known and unknown threats • Protects against sophisticated threats such as zero-day threats and rootkits • Helps ensure interoperability through the turnkey package vs. disparate point products
Advanced Rootkit Detection and Removal	<ul style="list-style-type: none"> • Provides superior rootkit detection and removal by integrating VxMS (Veritas Mapping Service, a Veritas technology.) This provides access below the operating system to allow thorough analysis and repair. 	<ul style="list-style-type: none"> • Detects and removes the most difficult rootkits that other vendors miss • Saves time, money and lost productivity associated with having to re-image infected machines
Generic Exploit Blocking	<ul style="list-style-type: none"> • Generic Exploit Blocking prevents entry of new threats at the network layer using a vulnerability-based Intrusion Prevention Solution¹ 	<ul style="list-style-type: none"> • Blocks all new exploits (including variants) of a vulnerability with a single signature • Blocks malware BEFORE it can enter a system
Deep Packet Inspection	<ul style="list-style-type: none"> • Provides administrators with the ability to create custom intrusion prevention signatures. Administrators can create custom, rule-based signatures to tailor the level of protection to their environment. 	<ul style="list-style-type: none"> • Blocks malware before it can enter a system • Gives administrators complete control to manage intrusion prevention signatures and tailor the level of protection for their environment
Proactive Threat Scan	<ul style="list-style-type: none"> • Provides behavioral-based protection (a WholeSecurity technology) unlike all other heuristic-based technologies with its Proactive Threat Scan scores both good and bad behaviors of unknown applications 	<ul style="list-style-type: none"> • Accurately detects malware without the need to set-up rule-based configurations or the worries of false positives • Provides more accurate detection of malware
Application Control	<ul style="list-style-type: none"> • Allows administrators to control access to specific processes, files and folders by users / applications • Provides application analysis, process control, file and registry access control, module and DLL control 	<ul style="list-style-type: none"> • Helps prevent malware from spreading or doing harm to the endpoint • Locks down endpoints to prevent data leakage • Enables administrators to restrict certain activities deemed suspicious or high risk
Device Control	<ul style="list-style-type: none"> • Controls which peripherals can be connected to a machine and how they are used plus locks down an endpoint by preventing thumb drives, CD burners, printers and other USB devices from connecting 	<ul style="list-style-type: none"> • Helps prevent sensitive and confidential data from being extracted or stolen from endpoints (data leakage) • Helps prevent endpoints from being infected by viruses spread from peripheral devices
Single Agent	<ul style="list-style-type: none"> • Delivers a single agent download for all Symantec 	<ul style="list-style-type: none"> • Lowers TCO for endpoint security

¹ Note: Originally introduced in Symantec Client Security



FEATURE	DESCRIPTION	BENEFIT
	<ul style="list-style-type: none"> Endpoint Protection technologies and the Symantec Network Access Control product Provides operational efficiencies such as single software and single policy updates 	<ul style="list-style-type: none"> Reduces administrative burden Offers unified and central reporting, licensing and maintenance Requires no change to the client when adding Symantec Network Access Control enforcement
Single Management Console	<ul style="list-style-type: none"> Delivers a single integrated interface for managing all Symantec Endpoint Protection technologies and the Symantec Network Access Control product while allowing a single communication method and content delivery system across all technologies Provides operational efficiencies such as single software and single policy updates 	<ul style="list-style-type: none"> Lowers TCO for endpoint security Reduces administrative burden Offers unified and central reporting, licensing and maintenance Requires no change to the client when adding Symantec Network Access Control enforcement
Simplified Client Interface	<ul style="list-style-type: none"> Offers customizable interface Gives administrators lock out configuration options from the end-user or can completely hide the interface 	<ul style="list-style-type: none"> Increases administrative control Offers user-friendly-Intuitive navigation
Active Directory Support	<ul style="list-style-type: none"> Symantec Endpoint Protection management supports importing Organization Units from Active Directory Offers group structures of users, computers and servers that can be imported and synchronized with the NT Domain, Active Directory and/or LDAP 	<ul style="list-style-type: none"> Reduces administrative effort Increases operational efficiencies
Roles-based Administration	<ul style="list-style-type: none"> Allows different administrators to be given different levels of access to the management system 	<ul style="list-style-type: none"> Offers flexible management Increases operational efficiencies
Patch Management & Distribution	<ul style="list-style-type: none"> Determines patches necessary for every Symantec Endpoint Protection client and automatically generates appropriate patch downloads 	<ul style="list-style-type: none"> Reduces administrative effort Includes tools for rolling patches out to Symantec Endpoint Protection clients Provides operational efficiencies
Integration with Altiris Endpoint Management Solutions	<ul style="list-style-type: none"> Allows easy distribution of client software packages, migrate older Symantec AntiVirus or other antivirus deployments and view deployment status and rollout activity 	<ul style="list-style-type: none"> Makes migration to next generation easy Reduces and simplifies deployment effort Provides enhanced visibility and control over migration and deployment activities and tasks
(Optional) Network Access Control	<ul style="list-style-type: none"> Symantec Endpoint Protection is Symantec Network Access Control ready and can be easily activated when the separate enforcement method is purchased without having to deploy additional agents or management consoles 	<ul style="list-style-type: none"> Provides a single platform to manage endpoint protection and endpoint compliance
Symantec Mobile Antivirus Feature	<ul style="list-style-type: none"> Enables secure mobile computing by providing comprehensive virus protection against malicious threats that target Windows® Mobile operating systems 	<ul style="list-style-type: none"> Provides on-device, automatic, real-time scanning that protects against threats downloaded from the Web, sent via email or a Wi-Fi connection, or received via Bluetooth or infrared ports Real-time Auto-Protect prevents users from ever accessing an infected file. When a threat is found, the product will automatically repair, quarantine or delete the threat to enable simple virus management and removal. Wireless LiveUpdate ensures up-to-date virus definitions
Brightmail - based Antispam Technology	<ul style="list-style-type: none"> Catches over 97 percent of spam, and less than one in a million false positives Delivers automatic spam rule updates Provides real-time analytics and reporting 	<ul style="list-style-type: none"> Protects messaging infrastructure and helps ensure business uptime and user productivity by reducing spam volume and keeping email secure Easy to manage and reduces administration costs
Zero-Day AV Protection	<ul style="list-style-type: none"> Proactively detects and quarantines suspicious messages before definitions become available 	<ul style="list-style-type: none"> Malware from email and IM is removed before it reaches mail servers Reduces the risk of downtime and business interruption due to virus related
Premium Content Control	<ul style="list-style-type: none"> Supports policies that can distinguish between live data and historical data Manages risks associated with data leakage, internal 	<ul style="list-style-type: none"> Provides comprehensive audit controls Extends protection of sensitive data



FEATURE	DESCRIPTION	BENEFIT
	governance, and compliance with specific regulations <ul style="list-style-type: none"> Provides powerful workflow tools, enabling better response to policy violations 	<ul style="list-style-type: none"> Reduces security risks and ensures sensitive data does not get transferred outside of the company

QUESTIONS TO CONSIDER

- What are you doing to effectively secure and manage your desktops, laptops, and servers?
- How does your current solution address zero-day threats?
- Are you operating in predominantly Mac or Linux Environment? If not, do you operate in a mixed or heterogeneous environment?
- Is your organization looking to lower IT costs and increase productivity?
- Would it benefit your organization to work with a vendor who can provide a unified yet comprehensive security solution, instead of dealing with multiple vendors and taking a piecemeal approach to security?

CLIENT / OS SUPPORT

The following operating systems are supported with Symantec Multi-tier Protection 11.0.2.

SYMANTEC ENDPOINT PROTECTION MANAGER, CONSOLE, AND DATABASE

Table 1 lists the minimum requirements for the computers on which to install the Symantec Endpoint Protection Manager and Console, and the database.

Component	32-bit	64-bit
Processor	1 GHz Intel Pentium III	1 GHz on x64 only with the following processors: <ul style="list-style-type: none"> Intel Xeon with Intel EM64T support Intel Pentium IV with EM 64T support AMD 64-bit Opteron™ AMD 64-bit Athlon™ Note: Itanium is not supported.
Operating System	The following operating systems are supported: <ul style="list-style-type: none"> Windows® 2000 Server/Advanced Server/Datacenter Server/Small Business Server with Service Pack 3 or later Windows XP Professional with Service Pack 1 or later Note: Windows XP supports a limited number of concurrent users if the clients are in "push" mode. Use "pull" mode on Windows XP servers for up to 100 clients. For more information, search for Symantec Endpoint Protection Manager 11.x communication troubleshooting on the Symantec Support Web Site . <ul style="list-style-type: none"> Windows Server 2003 Standard Edition/Enterprise Edition/Datacenter Edition/Storage Edition/Web Edition/Small Business Server 	The following operating systems are supported: <ul style="list-style-type: none"> Windows XP Professional x64 Edition with Service Pack 1 or later Windows Server 2003 Standard x64 Edition / Enterprise x64 Edition / Datacenter x64 Edition with Service Pack 1 or later Windows Compute Cluster Server 2003 Windows Storage Server 2003 Note: If you use Microsoft Clustering services for the Symantec Endpoint Protection Manager server you must install the Symantec Endpoint Protection Manager on the local volume.
Memory	1 GB RAM minimum (2-4 GB recommended)	1 GB RAM minimum (2-4 GB recommended)
Hard Disk	4 GB for the server, plus an additional 4 GB for the database	4 GB for the server, plus an additional 4 GB for the database
Display	Super VGA (1,024x768) or higher-resolution video adapter and monitor	Super VGA (1,024x768) or higher-resolution video adapter and monitor
Database	The Symantec Endpoint Protection Manager includes an embedded database. You may also choose to use one of the following versions of Microsoft SQL Server: <ul style="list-style-type: none"> Microsoft SQL Server 2000 with Service Pack 3 or later Microsoft SQL Server 2005 Note: Microsoft SQL Server is optional.	The Symantec Endpoint Protection Manager includes an embedded database. You may also choose to use one of the following versions of Microsoft SQL Server: <ul style="list-style-type: none"> Microsoft SQL Server 2000 with Service Pack 3 or later Microsoft SQL Server 2005 Note: Microsoft SQL Server is optional.
Other Requirements	The following other requirements must be met: <ul style="list-style-type: none"> Internet Information Services server 5.0 or later with World Wide Web services enabled Internet Explorer 6.0 or later Static IP address (recommended) 	The following other requirements must be met: <ul style="list-style-type: none"> Internet Information Services server 5.0 or later with World Wide Web services enabled Internet Explorer 6.0 or later Static IP address (recommended)



Symantec Endpoint Protection Manager and Console

Table 2 lists the minimum requirements for the computers on which to install the Symantec Endpoint Protection Manager and Console.

Component	32-bit	64-bit
Processor	1 GHz Intel Pentium III	<ul style="list-style-type: none"> 1 GHz on x64 only with the following processors: Intel Xeon with Intel EM64T support Intel Pentium IV with EM64T support AMD 64-bit Opteron™ AMD 64-bit Athlon™ <p>Note: Itanium is not supported.</p>
Operating System	<ul style="list-style-type: none"> The following operating systems are supported: Windows® 2000 Server/Advanced Server/Datacenter Server with Service Pack 3 or later Windows XP Professional with Service Pack 1 or later <p>Note: Windows XP supports a limited number of concurrent users if the clients are in "push" mode. Use "pull" mode on Windows XP servers for up to 100 clients. For more information, search for Symantec Endpoint Protection Manager 11.x communication troubleshooting on the Symantec Support Web Site.</p> <ul style="list-style-type: none"> Windows Server 2003 Standard Edition/Enterprise Edition/Datacenter Edition/Web Edition/Small Business Server 	<ul style="list-style-type: none"> The following operating systems are supported: Windows XP Professional x64 Edition with Service Pack 1 or later Windows Server 2003 Standard x64 Edition/Enterprise x64 Edition/Datacenter x64 Edition with Service Pack 1 or later Windows Compute Cluster Server 2003 Windows Storage Server 2003 <p>Note: If you use Microsoft Clustering services for the SEPM server you must install the SEPM server on the local volume.</p>
Memory	1 GB of RAM minimum (2 GB recommended)	1 GB of RAM minimum (2 GB recommended)
Hard Disk	2 GB (4 GB recommended)	2 GB (4 GB recommended)
Display	Super VGA (1,024x768) or higher-resolution video adapter and monitor	Super VGA (1,024x768) or higher-resolution video adapter and monitor
Other Requirements	<ul style="list-style-type: none"> The following other requirements must be met: Internet Information Services server 5.0 or later with World Wide Web services enabled. Internet Explorer 6.0 or later Static IP address (recommended) 	<ul style="list-style-type: none"> The following other requirements must be met: Internet Information Services server 5.0 or later with World Wide Web services enabled. Internet Explorer 6.0 or later Static IP address (recommended)

Symantec Endpoint Protection Console

Table 3 lists the minimum requirements for the computers on which to install the Symantec Endpoint Protection Console.

Component	32-bit	64-bit
Processor	1 GHz Intel Pentium III	1 GHz on x64 only with the following processors: <ul style="list-style-type: none"> Intel Xeon with Intel EM64T support Intel Pentium IV with EM64T support AMD 64-bit Opteron™ AMD 64-bit Athlon™ <p>Note: Itanium is not supported.</p>
Operating System	The following operating systems are supported: <ul style="list-style-type: none"> Windows® 2000 Professional/Server/Advanced Server/Datacenter Server/Small Business Server with Service Pack 3 or later Windows XP Professional with Service Pack 1 or later <p>Note: Windows XP supports a limited number of concurrent users if the clients are in "push" mode. Use "pull" mode on Windows XP servers for up to 100 clients. For more information, search for Symantec Endpoint Protection Manager 11.x communication troubleshooting on the Symantec Support Web Site.</p> <ul style="list-style-type: none"> Windows Server 2003 Standard Edition/Enterprise Edition/Datacenter Edition/Web Edition/Small Business Server Windows Vista (x86) 	The following operating systems are supported: <ul style="list-style-type: none"> Windows XP Professional x64 Edition with Service Pack 1 or later Windows Server 2003 Standard x64 Edition / Enterprise x64 Edition / Datacenter x64 Edition with Service Pack 1 or later Windows Compute Cluster Server 2003 Windows Storage Server 2003 Windows Vista (x64) <p>Note: The Symantec Network Access Control installation CD contains a 64-bit application. If you use Microsoft Clustering services for the SEPM server you must install the SEPM server on the local volume.</p>
Memory	512 MB of RAM (1 GB recommended)	512 MB of RAM (1 GB recommended)



Component	32-bit	64-bit
Hard Disk	15 MB	15 MB
Display	Super VGA (1,024x768) or higher-resolution video adapter and monitor	Super VGA (1,024x768) or higher-resolution video adapter and monitor
Other Requirements	The following other requirements must be met: <ul style="list-style-type: none"> • Internet Explorer 6.0 or later • Java Runtime Environment 5.0, update 13 or above recommended 	The following other requirements must be met: <ul style="list-style-type: none"> • Internet Explorer 6.0 or later • Java Runtime Environment 5.0, update 13 or above recommended

Quarantine Console

Table 4 lists the minimum requirements for the computers on which to install the Quarantine Console.

Component	32-bit	64-bit
Processor	600 MHz Intel Pentium III	Not tested
Operating System	The following operating systems are Not tested supported: <ul style="list-style-type: none"> • Windows® 2000 Professional/Server/Advanced Server/Datacenter Server/Small Business Server with Service Pack 3 or later • Windows XP Professional with Service Pack 1 or later • Windows Server 2003 Standard Edition/Enterprise Edition/Datacenter Edition/Web Edition • Windows Vista (x86) Home Basic Edition/Home Premium Edition/Business Edition/Enterprise Edition/Ultimate Edition • Windows Server 2008 Standard Edition/Enterprise Edition/Datacenter Edition/Web Edition 	Not tested
Memory	64 MB of RAM	Not tested
Hard Disk	35 MB	Not tested
Display	Super VGA (1,024x768) or higher-resolution Not tested video adapter and monitor	Not tested
Other Requirements	The following other requirements must be met: <ul style="list-style-type: none"> • Internet Explorer 5.5 Service Pack 2 or later • Microsoft Management Console version 1.2 or later • If MMC is not already installed, you need 3 MB free disk space (10 MB during installation). 	Not tested

Central Quarantine Server

Table 5 lists the minimum requirements for the computers on which to install the Central Quarantine Server.

Component	32-bit	64-bit
Processor	600 MHz Intel Pentium III	Not tested
Operating System	The following operating systems are Not tested supported: <ul style="list-style-type: none"> • Windows® 2000 Professional/Server/Advanced Server/Datacenter Server/Small Business Server with Service Pack 3 or later • Windows XP Professional with Service Pack 1 or later • Windows Server 2003 Standard Edition/Enterprise Edition/Datacenter Edition/Web Edition • Windows Vista (x86) Home Basic Edition/Home Premium Edition/Business Edition/Enterprise Edition/Ultimate Edition 	Not tested
Memory	128 MB of RAM	Not tested
Hard Disk	40 MB, 500 MB to 4 GB recommended for quarantined items, and 250-MB swap file	Not tested

Component	32-bit	64-bit
Display	Super VGA (1,024x768) or higher-resolution video adapter and monitor	Not tested
Other Requirements	The following other requirements must be met: <ul style="list-style-type: none"> Internet Explorer 5.5 Service Pack 2 or later 	Not tested

Symantec Endpoint Protection

Table 6 lists the minimum requirements for the computers on which to install Symantec Endpoint Protection.

Component	32-bit	64-bit
Processor	400 MHz Intel Pentium III (1 GHz for Windows Vista)	1 GHz on x64 only with the following processors: <ul style="list-style-type: none"> Intel Xeon with Intel EM64T support Intel Pentium IV with EM64T support AMD 64-bit Opteron™ AMD 64-bit Athlon™ Note: Itanium is not supported.
Operating System	The following operating systems are supported: <ul style="list-style-type: none"> Windows® 2000 Professional/Server/Advanced Server/Datacenter Server/Small Business Server with Service Pack 3 or later Windows XP Home Edition/Professional with Service Pack 1 or later/Tablet PC Edition/Media Center Edition Windows Server 2003 Standard Edition/Enterprise Edition/Datacenter Edition/Web Edition/Small Business Server Windows Vista (x86) Home Basic Edition/Home Premium Edition/Business Edition/Enterprise Edition/Ultimate Edition Windows Server 2008 Standard Edition/Enterprise Edition/Datacenter Edition/Web Edition 	The following operating systems are supported: <ul style="list-style-type: none"> Windows XP Professional x64 Edition with Service Pack 1 or later Windows Server 2003 x64 Edition Windows Compute Cluster Server 2003 Windows Storage Server 2003 Windows Vista Home Basic x64 Edition/Home Premium x64 Edition/Business x64 Edition/Enterprise x64 Edition/Ultimate x64 Edition Windows Server 2008 Standard x64 Edition/Enterprise x64 Edition/ Datacenter x64 Edition/Web x64 Edition Note: If you are using Microsoft Clustering Services, you must install the client on the local volume.
Memory	256 MB of RAM	256 MB of RAM
Hard disk	600 MB	700 MB
Display	Super VGA (1,024x768) or higher-resolution video adapter and monitor	Super VGA (1,024x768) or higher-resolution video adapter and monitor
Other Requirements	Internet Explorer 6.0 or later Terminal Server clients connecting to a computer with antivirus protection have the following additional requirements: <ul style="list-style-type: none"> Microsoft Terminal Server RDP (Remote Desktop Protocol) client Citrix® Metaframe® (ICA) client 1.8 or later if using Citrix Metaframe server on Terminal Server 	Internet Explorer 6.0 or later

Symantec Brightmail Gateway

Table 7 lists the minimum requirements for the servers on which to install the Brightmail Gateway software Subscription.

Supported Internet Browsers	Application OS
Microsoft Internet Explorer 6.0	Linux-based operating system pre-hardened against common vulnerabilities and attacks
Microsoft Internet Explorer 7.0	
Firefox 2.0	
Recommended Deployment Options	
VMware Server 1.0.4	Demonstration, Test
VMware ESX Server 3.0.2	Production, Demonstration, Test

Symantec Mail Security for Microsoft Exchange

	Supported Operating Systems
Server Installation Requirements	Windows 2000 Server/Advanced Server/Data Center (SP4), Windows Server 2003 Standard/Enterprise/Data Center (SP1), Microsoft Windows Server 2003 or Windows Server 2003 R2,

	Supported Operating Systems
	Standard or Enterprise Edition, Microsoft Windows Server 2008 x64 Standard or Enterprise Edition
Console-only Installation System Requirements	<ul style="list-style-type: none"> Windows 2000 (SP4), Windows 2003 (SP1), Windows XP (SP1)
Exchange Server 2007 Deployments	<ul style="list-style-type: none"> x64 architecture-based computer with Intel processor that supports Intel Extended Memory 64 technology (Intel EM64T), or AMD processor that supports the AMD64 platform 2 GB RAM minimum

Symantec Mail Security for Domino

System requirements

- Lotus Domino® server version 6.5.x or 7.x
- Microsoft® Windows® 2000 Server, Windows 2000 Advanced Server, Windows Server 2003, or Windows Server 2003 Enterprise Edition

Lotus Notes® client requirements

- Lotus Notes version 6.5.x or 7.x
- 128 MB RAM minimum (256 MB or more recommended)
- 300 MB available disk space

- NOTE:** Domino server should be sized based on Domino system requirements. System requirements should take into account additional needs such as file system antivirus protection, backup operations, and other business-critical applications unique to the environment.

Symantec AntiVirus for Macintosh 10.2 Administration Server

	Requirements
Operating System	Mac OS X Server 10.4.11 – 10.5x
Hardware	<ul style="list-style-type: none"> Xserve G5, Xserve, Power Mac G5, Power Mac G4, Macintosh Server G4, Power Macintosh G3 (Blue & White), Macintosh Server G3 (Blue & White), iMac, eMac or Mac mini computer 256 MB of RAM, at least 512 MB of RAM for high-demand servers running multiple services Built-in FireWire 4 GB of available disk space
Other Software	<ul style="list-style-type: none"> As an included add-on component, the Symantec Administration Console requires that Macintosh clients with Symantec AntiVirus 10.2 for Macintosh run under Mac OS 10.4.11 -10.5.x.

NOTE: Mac OS X Server 10.4.11 - 10.5.x is required. Mac OS X Server 10.4 and 10.5 software include Apache and MySQL.

Symantec AntiVirus for Macintosh 10.2 Administration Console

	Supported
Administration Console Browsers	<ul style="list-style-type: none"> Mac OS X + Safari 1.2.X, Firefox 2 Windows XP Pro + Internet Explorer 6 SP2, Firefox 2 RedHat Linux + Netscape 7

Symantec AntiVirus for Macintosh Client 10.2

	Requirements
Operating System	Mac OS X Server 10.4.11 – 10.5x
Hardware	<ul style="list-style-type: none"> G3 processor or higher (G4 800 MHz or better if running Mac OS X 10.4.11 or Mac OS X 10.5.x) 192 MB of RAM 40 MB of available hard disk space for installation Internet connection required for LiveUpdate

Copyright © 2008 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 United States and other countries. Other names may be trademarks of their respective owners.