



Symantec™ Endpoint Protection 11.0

OVERVIEW

Symantec™ Endpoint Protection replaces Symantec AntiVirus Corporate Edition, Symantec Client Security, Symantec Sygate Enterprise protection and Confidence Online for PCs. Symantec Endpoint Protection combines Symantec AntiVirus™ with advanced threat prevention to deliver unmatched defense against malware for laptops, desktops and servers. It delivers the most advanced technology available to protect from 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 secure data. Symantec Endpoint Protection seamlessly integrates these essential security capabilities in a single agent and single console to reduce costs, complexity and administrative overhead associated with managing multiple endpoint security products.

Symantec Endpoint Protection Product Family

	SYMANTEC ENDPOINT PROTECTION	SYMANTEC ENDPOINT 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 Control	X	X	X
Symantec Mail Security for Microsoft Exchange		X	X
Symantec Mail Security for Domino			X
Symantec Mail Security for SMTP			X

Gray area = centrally managed via a single agent and single console

TARGET MARKET

Primary – Large/Medium Enterprise (1,000-10,000+ employees)

Secondary – Small/Medium Enterprise (10-999 employees)

IT Challenges: Reduce rising costs and manage complexity associated with acquiring and managing multiple endpoint security technologies. Maintain control over endpoint security protection as threats become more sophisticated and targeted at endpoint devices. Supplement signature-based solutions (like antivirus) with proactive non-signature-based security protection mechanisms. Protect against increasing levels of email-borne threats and spam, in addition to protecting non-windows devices.

Business / Legal Challenges: Meet end-user demand to increase productivity by accessing the network remotely (VPN, web-based telecommuting, unmanaged devices) while providing protection due to increased exposure risks.

Industry Segments: Customers span all industry segments.

SALES OPPORTUNITIES

CUSTOMER PAIN POINTS	DECISION MAKER	HOW WE DELIVER
Complex Endpoint Security Environments	<ul style="list-style-type: none"> • Strategic Security: CSO / CISO / Security Architect • Strategic IT: CTO / CIO / VP /Dir IT / Infra / Ops • Functional IT: IT Mgmt / Ops / Storage/Network / Desktop / Server Mgrs 	<ul style="list-style-type: none"> • Combines essential endpoint security technologies • Offers a single management console reducing administrative burden
Protect Data, Email and Non-window Devices from Growing Threats	<ul style="list-style-type: none"> • Strategic Security: CSO / CISO / Security Architect • Functional IT: IT Mgmt / Ops / Storage/Network / Desktop / Server Mgrs 	<ul style="list-style-type: none"> • Provides advanced threat prevention protecting from both known and unknown threats
Reduce Costs Associated with Managing Multiple	<ul style="list-style-type: none"> • Strategic Business: CEO / CFO / COO • Strategic IT: CTO / CIO / VP /Dir IT / Infra / Ops 	<ul style="list-style-type: none"> • Reduces procurement, support and maintenance costs utilizing a single



Symantec™ Endpoint Protection 11.0

CUSTOMER PAIN POINTS	DECISION MAKER	HOW WE DELIVER
Endpoint Security Solutions	<ul style="list-style-type: none"> • Functional IT: IT Mgmt / Ops / Storage/Network / Desktop / Server Mgrs 	agent and single management console
Prove Internal and External Regulation / Compliance with Security Policies	<ul style="list-style-type: none"> • Strategic Business: CEO / CFO / COO • Strategic Security: CSO / CISO / Security Architect • Functional IT: IT Mgmt / Ops / Storage/Network / Desktop / Server Mgrs • Functional Business: Compliance Officer / Audit / LOB 	<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)

PARTNER OPPORTUNITIES

CUSTOMER PAIN POINTS	HOW WE DELIVER
Improves Profitability	<ul style="list-style-type: none"> • Partners up-selling Symantec Endpoint Protection 11.0 with the Essential maintenance plan can increase their revenue while providing more support & satisfaction to their customers • Leverages the new competitive cross-grade pricing to sell Symantec Endpoint Protection 11.0 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 Symantec AntiVirus customers from the Express buying program 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 Endpoint Protection 11.0
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

SOLUTION MAPPING

Solution Selling

Symantec Endpoint Protection delivers unmatched protection from even the most sophisticated attacks by combining Symantec AntiVirus technology with advanced threat prevention and simplifying endpoint security administration so that customers can save time and money while protecting assets and business. Unlike our competitors, Symantec Endpoint Protection offers proven world class protection in a single agent without added resource overhead so that customers can efficiently manage endpoint security and gain confidence that corporate assets and business are protected. Symantec Endpoint Protection can be combined with a variety of Symantec products that provide scalable selling opportunities within the following solutions:

- **IT Policy Compliance:** provides a common set of management tools necessary to help manage IT compliance processes governing the confidentiality, availability, and integrity of regulated information in a proactive, continuous, and efficient manner
- **Enterprise Security:** peer products within the Endpoint Security, Security Management, and Messaging Security product lines will share buying centers with Symantec Endpoint Protection that will have similar pain points and IT risk management goals
- **Global Consulting and Education Services:** for training, assessment, design and deployment

Cross-sell/Up-sell Opportunities

- **Symantec Network Access Control:** Symantec Endpoint Protection and Symantec Network Access Control utilize the same agent and the same management console providing organizations with the tools needed to reduce administrative burden and lower total cost of ownership for endpoint security.
- **Symantec Critical System Protection:** For environments containing additional server operating systems, beyond those currently supported in Symantec Endpoint Protection, Symantec Critical System Protection offers protection capabilities such as Intrusion Prevention for UNIX and Linux OSs; in addition to the Windows Server.





Symantec™ Endpoint Protection 11.0

- **Symantec Mobile Security Suite:** Version 5.0 extends protection and compliance capabilities out to Windows Mobile devices Offering Symantec AntiVirus for non-Windows Mobile devices like Symbian and Palm OS.
- **Symantec On-Demand Protection Solution:** Extends endpoint protection out to unmanaged devices by protecting systems accessing web-enabled applications, such as web mail (MS Outlook Web Access), and the data moved onto the endpoints during the user sessions.

KEY FEATURES AND BENEFITS

What's New in Symantec Endpoint Protection 11.0?

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 and proactive protection with the ability to enable the pieces you need, as you need them 	<ul style="list-style-type: none"> • 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
Raw Disk Scan	<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 unique 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 	<ul style="list-style-type: none"> • 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"> • Behavioral-based protection (a WholeSecurity technology) unlike all other heuristic-based technologies 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"> • Prevents 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"> • Prevents sensitive and confidential data from being extracted or stolen from endpoints (data leakage) • Prevents endpoints from being infected by viruses spread from peripheral devices
Single Agent	<ul style="list-style-type: none"> • Delivers a single management agent for all Symantec Endpoint Protection technologies and the Symantec Network Access Control product • Provides operation efficiencies such as single software and single policy updates 	<ul style="list-style-type: none"> • Lowers total cost of ownership 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
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 	<ul style="list-style-type: none"> • Lowers total cost of ownership 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

¹ Note: Originally introduced in Symantec Client Security



Symantec™ Endpoint Protection 11.0

FEATURE	DESCRIPTION	BENEFIT
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"> Administrative control User friendly Intuitive navigation
Active Directory Support	<ul style="list-style-type: none"> Symantec Endpoint Protection management supports importing Organization Units from Active Directory Group structures of users, computers and servers 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 and 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
(Optional) Symantec 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"> Single platform to manage endpoint protection and endpoint compliance

QUALIFYING QUESTIONS

1. Are security threats posing increasing risks to your organizations brand and reputation?
2. Are you having challenges managing multiple endpoint security products with separate management consoles?
3. Are your endpoint security solutions becoming more costly and complex to manage?
4. Do you find it difficult to stay ahead of security threats while sustaining compliance to internal IT policies and regulatory mandates?
5. Do you allow your end users access into your network via remote, VPN, web-based, telecommuting or from non-company unmanaged devices?
6. Has your organization faced financial loss due to security breaches?
7. What are your Microsoft Vista deployment plans?

COMPETITION

For additional in-depth competitive information on these organizations and others, please refer to the SCORE page.

COMPETITION	KEY DIFFERENTIATORS
Microsoft	<ul style="list-style-type: none"> Symantec AntiVirus technology has not failed a single VB100 test since 1999 – Microsoft was tested only twice and failed the last Symantec provides proven security while MS ForeFront Client Security is a 1.0 product based on technology that has proven to be insecure Symantec is a dedicated security company and has built a complete security infrastructure over many years – security at Microsoft is just a small piece of the business The Intrusion Prevention System functionality in Symantec Endpoint Protection stops malware at the network level before it infects the endpoint Generic Exploit Blocking provides protection from known and unknown threats that attack vulnerabilities BEFORE Microsoft provides patches Symantec detects and removes rootkits faster than MS Windows Defender Symantec protects across platforms & form factors while Microsoft only provides a point solution for PCs
McAfee	<ul style="list-style-type: none"> To achieve Symantec Endpoint Protection levels you would have to install 6 McAfee products/modules/agents on the client Symantec AntiVirus technology has protected its users since 1999 against viruses that are in the wild – McAfee has failed the VB100 test 12 times (in the same time, last time in February 2006) The Firewall integrated in Symantec Endpoint Protection is Sygate FW based – leading the Gartner Magic Quadrant



Symantec™ Endpoint Protection 11.0

COMPETITION	KEY DIFFERENTIATORS
	<p>since 2001, while McAfee is a considered a niche player</p> <ul style="list-style-type: none"> • Symantec Endpoint Protection customers can create their own Network IPS rules using a SNORT-like Syntax and can create their own HIPS rules using a build-in-rule editor • Symantec Endpoint Protection includes technology from Veritas to detect rootkits on a lower level – part of the consumer product that is proven to be the most effective on the market
<p>Trend Micro</p>	<ul style="list-style-type: none"> • Symantec protects against unknown threats with technologies that do not requires signatures • Symantec AntiVirus technology has been protecting users since 1999 against viruses that are in the wild – Trend Micro has failed the VB100 test 3 times (in the same time, last time in December 2006) • The Firewall integrated in Symantec Endpoint Protection is Sygate FW based – leading the Gartner Magic Quadrant since 2001 • Symantec Endpoint Protection includes technology from Veritas to detect rootkits on a lower level – part of the consumer product that is proven to be the most effective on the market • Generic Exploit Blocking protects against unknown threats and variants by shielding vulnerabilities before a patch is available or deployed • 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 • Symantec's Advanced Protection provides more reports, customized notifications, integration with syslog than other 3rd party products

Copyright © 2007 Symantec Corporation. All rights reserved. Symantec and the Symantec logo 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.