



Symantec™ Multi-Tier Protection 11

Comprehensive virus protection for workstations and network servers enterprise-wide

- Multi-layered Protection
- Generic Exploit Blocking
- Proactive Threat Scan
- Application Control
- Device Control
- Mail Protection
- Sygate Firewall with IPS
- Single Management Console
- Simplified client Interface
- Roles-based Administration



معرفی

Symantec Endpoint Protection ترکیبی است از یک ضد ویروس هوشمند همراه با پیشرفته‌ترین روش مقابله با ویروسها که توانایی مقابله با پیچیده‌ترین حملات ویروسی که در روشهای سنتی قابل مقابله نیستند را دارد. این نرم افزار با روشهای پیشرفته شناسایی "مبتنی بر رفتار" خود قابلیت مقابله با ویروسها و حملاتی را دارد که حتی برای اولین بار مشاهده می‌شوند. مثل حملات Zero-day و Rootkitها. این ضد ویروس همچنین شامل فایروال در سطح کلاینتها همراه با سیستم ضد حمله IPS بوده و نیز مجهز به سیستم کنترل سخت افزار (Device Control) می‌باشد که توانایی فعال یا غیر فعال کردن سخت افزارهای سیستمی مثل USB، CD/DVD و کارت شبکه و کارت صدا و.... را بر روی کلاینتها را دارد. این نرم افزار قابلیت محافظت از میل سرورهایی چون Microsoft Exchange و SMTP Mail Server و Domino را نیز دارد که توانایی چون جلوگیری از ورود و خروج ویروس، هرزنامه(در صورت خرید Premium Add-on) و همچنین کنترل محتوی و مدیریت فایل‌های ضمیمه و اعمال مختلف سیاستها را بر روی Mail Server دارا می‌باشد.

ویژگیهای برجسته:

• Proactive Protection

در این روش محافظت و شناسایی جدید که از تکنولوژی منحصر به فرد Symantec استفاده می‌کند ویروسها و حملات مخرب براساس رفتارشان شناسایی می‌شوند. اگر رفتار یک برنامه مخرب تشخیص داده شد، به صورت هوشمند آن برنامه توسط ضد ویروس در یک محیط امن اجرا شده و تمام رفتارش ثبت می‌شود و بر اساس آن الگوریتم مقابله با آن ساخته می‌شود. در نتیجه نیازی نیست که حتماً ویروس یا برنامه مخرب از قبل در بانک اطلاعاتی ضد ویروس وجود داشته باشد، در نتیجه جدیدترین ویروسها را در بدو ساخته شدن شناسایی می‌کند حتی در صورتیکه ضد ویروس بروز نشده باشد.



- دیواره آتش Firewall به همراه IPS این نرم افزار دارای دیواره آتش همراه با سیستم جلوگیری از حمله (IPS) و قابلیت کنترل دسترسی و اجرای Application ها و برنامه های کاربردی بر روی ایستگاههای کاری می باشد.
- قابلیت محافظت و کنترل دسترسی به قطعات مختلف کامپیوتر با این ابزار شما قادر خواهید بود دسترسی به اجزاء مختلف کامپیوتر خود و یا کاربران را مدیریت کنید. بدین صورت که چه قطعاتی بر روی کامپیوتر مربوطه فعال یا غیرفعال باشد مثلاً USB ها کارت های شبکه، مودم، کارت صدا، CD/DVD درایوها، Keyboard، Mouse، هارد درایو و بسیاری موارد دیگر. همچنین قادر خواهید بود از بین این قطعات برای آنها استثنا هم قائل شوید مثلاً USB Printer و یا Scanner را از سایر USB ها جدا نمایید تا فعال بوده و بقیه USB ها غیرفعال باشند.
- سیستم گزارش گیری پیشرفته گرافیکی در این نرم افزار که همزمان با نصب سرور نصب می شود، شما یک سیستم گزارش گیری پیشرفته دارید که هم بصورت Web-based و هم از طریق کنسول مدیریتی ضد ویروس قابل اجرا است.
- پشتیبانی از ایستگاههای کاری Linux و Macintosh و Novell
- نصب و بروزرسانی و مدیریت متمرکز از راه دور توسط یک کنسول واحد برای تمام امکانات برنامه
- جلوگیری از سوء استفاده و نفوذ کدهای مخرب (Exploit Blocking)
- بازرسی دقیق درون Packet ها
- استفاده از فقط یک Agent برای تمام امکانات برنامه همراه با رابط کاربری ساده و زیبا
- محافظت از ورود Spyware ها و Adware ها و قابلیت شناسایی به محض ورود به سیستم
- قابلیت دفاع از خود در برابر حملات مخرب (Tamper Protection)
- ترمیم و بازگرداندن تغییرات انجام شده توسط ویروسها و Spyware ها در Registry و Browser و ...
- بهبود در چک کردن فایل های روی شبکه جهت ممانعت از چک شدن تکراری یک فایل در انتقال از روی شبکه
- قابلیت شناسایی Email ها و پاکسازی آنها از سرور
- قابلیت محافظت از Outlook
- قابلیت بروزرشدن مداوم و اتوماتیک حتی هر ۳۰ دقیقه یکبار
- قابلیت ایجاد قرنطینه مرکزی
- قابلیت ایجاد سرور بروزرسانی مرکزی داخلی
- قابلیت مانیتورینگ پیشرفته
- سرعت بالا و کمترین استفاده از منابع سیستم مثل Memory و CPU
- کمترین تاثیر منفی در سرعت کار کاربران نسبت به محصولات مشابه
- ایجاد قرنطینه مرکزی فایل های آلوده و استخراج فایل های سالم از بین آنها
- امکان شناسایی Email های آلوده در سطح کامپیوترهای کاربران
- امکان اختصاص چند سرور برای توزیع بار ایستگاه های کاری یا بعنوان Secondary ضد ویروس



- محافظت از حذف ضد ویروس و تغییر تنظیمات در ایستگاه‌های کاری توسط کاربران
- بروزرسانی ایستگاه‌های کاری از طریق سرور به صورت اتوماتیک با زمان‌بندی دلخواه
- ارائه Logها و گزارشات مفید در مورد ویروس‌های پیدا شده در شبکه و وضعیت ضد ویروس‌های موجود در ایستگاه‌های کاری
- قابلیت اعمال سیاست‌های کاری (Policy) در زمینه ضد ویروس (مثل پنهان کردن آیکون ضد ویروس از دید کاربر، جلوگیری از دسترسی کاربران به تنظیمات ضد ویروس کامپیوترهایشان، تعیین تنظیمات ضد ویروس و زمان‌های بروزرسانی ضد ویروس‌های موجود در ایستگاه‌های کاری از راه دور)
- شناسایی Emailهای آلوده و جلوگیری از ورود آنها به سرور
- ضد Spam جامع و هوشمند (در صورت خرید Premium Add-on)
- پاکسازی کامل محتوای تمام نامه‌ها (متن و پیوست)
- پاکسازی نامه‌ها بوسیله نام، اندازه، نوع محتوا و پیوستها

مقایسه محصولات

Symantec Endpoint Protection Product Family

	Symantec Endpoint Protection	Symantec Multi-tier Protection
Antivirus	x	x
Antispyware	x	x
Desktop Firewall	x	x
Intrusion Prevention	x	x
Device Control	x	x
Symantec Mail Security for Microsoft Exchange		x
Symantec Mail Security for Domino		x
Symantec Mail Security for SMTP		x
Client for Linux		x
Client for Macintosh		x



Minimum system requirement:

Symantec Endpoint Protection Client

Protection software for server, desktop, and laptop system

Component	32-bit	64-bit
Microsoft Windows Vista	x	x
Microsoft Windows 2003	x	x
Microsoft Windows XP	x	x
Microsoft Windows 2000 (SP3 and later)	x	
Processor	400 MHz	1 GHz
Memory	256 MB of RAM	256 MB of RAM
Hard Disk	600 MB	700 MB

Symantec Endpoint Protection Manager

Central Administration server

Component	32-bit	64-bit
Microsoft Windows 2003	x	x
Microsoft Windows XP	x	
Microsoft Windows 2000 (SP3 and later)	x	
Processor	600 MHz	1 GHz
Memory	512 MB of RAM	512 MB of RAM
Hard Disk	500 MB	500 MB



**Symantec Endpoint Protection Console
Remote Administration Console (optional)**

Component	32-bit	64-bit
Microsoft Windows Vista	x	x
Microsoft Windows 2003	x	x
Microsoft Windows XP	x	x
Microsoft Windows 2000 (SP3 and later)	x	
Processor	600 MHz	1 GHz
Memory	512 MB of RAM	512 MB of RAM
Hard Disk	500 MB	500 MB

**Symantec Antivirus for Linux Client
Linux Distribution Supported:**

Component	32-bit	64-bit
Red Hat enterprise Linux	x	
SUSE Linux Enterprise (Server/Desktop)	x	
Novel Open Enterprise Server	x	
VMVare ESX	x	



Symantec Endpoint Protection	Symantec Multi-tier Protection	Symantec Mail Security for Microsoft Exchange	Symantec Mail Security for SMTP	ویژگی‌ها
X	X			قابلیت محافظت هوشمند بر اساس رفتار Proactive
X	X	X	X	عکس العمل سریع در هنگام بروز خطر
X	X			قابلیت محافظت از خود در برابر کدهای مخرب
X	X	X	X	قابلیت شناسایی Adwareها و Spywareها به محض ورود به سیستم
X	X			قابلیت فعال یا غیر فعال نمودن قطعات سخت افزاری ایستگاههای کاری به دلخواه
X	X			قابلیت جلوگیری از اجرای برنامه‌ها یا دسترسی آنها به اینترنت
X	X			شناسایی Emailهای آلوده و جلوگیری از ورود آنها به ایستگاههای کاری از طریق Outlook
X	X			بررسی حافظه و از بین بردن برنامه‌های مقیم مشکوک
	X	X	X	شناسایی Emailهای آلوده و جلوگیری از ورود آنها به سرور
	X	X	X	ضد Spam جامع و هوشمند (در صورت خرید Premium Add-on)
	X	X	X	پاکسازی کامل محتوای تمام نامه‌ها (متن و پیوست)
	X	X		پاکسازی نامه‌ها بوسیله نام، اندازه، نوع محتوا و پیوستها
X	X			برقراری امنیت کامل بوسیله فایروال در سطح برنامه‌های کاربردی
X	X			جلوگیری از هکرها و حمله‌های اینترنتی
X	X			سیستم جلوگیری از حمله در سطح ایستگاههای کاری (IPS)
	X			پشتیبانی از سیستم عامل Linux
X	X			پشتیبانی از سیستم عامل Novell
	X			پشتیبانی از سیستم عامل Macintosh