- دقت تشخیص بالای ۹۹٪ اسپم و بدافزار
- حفظ بهره وری کارمندان و اعتبار شرکت/سازمان
- محافظت از ایمیل های ورودی و خروجی
- مدیریت ساده و متمرکز با کنسول وب
- تلفیق با Symantec Encryption و Symantec DLP برای رمزگذاری ایمیل ها و جلوگیری از نشت اطلاعات حیاتی و اعتباری سازمان/شرکت
- محافظت در برابر حمله هدفمند و تهدیدات روز صفر
- تبیین قوانین کنترلی توسط مدیر سیستم
- قابلیت نصب به صورت ماشین مجازی
- گزارش دهی جامع با بیش از ۵۰ گزارش از پیش تعیین شده

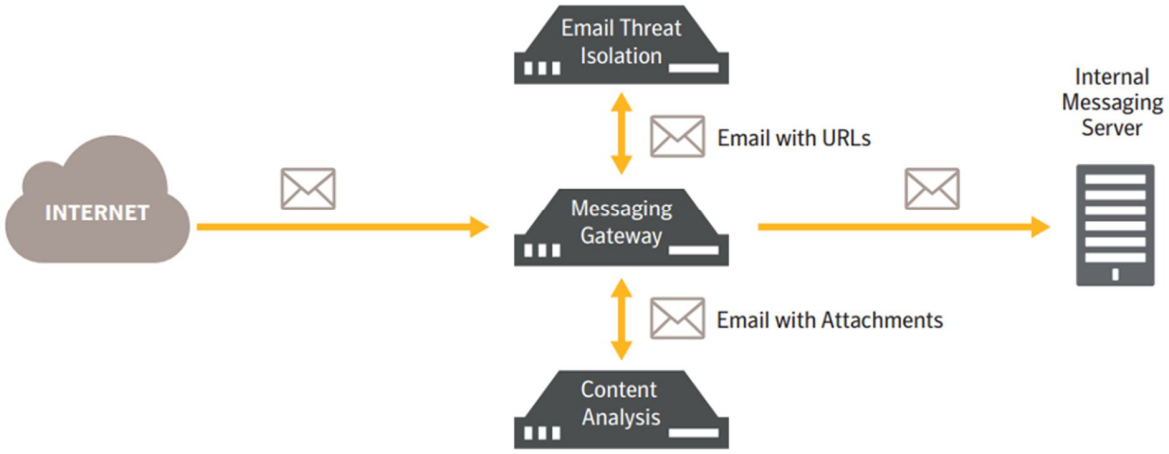
بررسی اجمالی

Symantec Messaging Gateway و یا به اختصار SMG ، محصولی از غول امنیتی جهان یعنی سیمانتک به منظور تامین امنیت ایمیل سازمانی/شرکتی می‌باشد. SMG، شرکتها/سازمان ها را قادر می‌سازد تا زیرساخت های ایمیل خود را با روشهایی مانند: محافظت آنتی اسپم و ضد بدافزار بلادرنگ موثر و دقیق، محافظت در برابر حملات هدفمند، فیلتر کردن پیشرفته محتوا، DLP و رمزگذاری ایمیل ایمن سازند. مدیریت این محصول ساده بوده و بیش از ۹۹ درصد اسپم ها را با کمتر از یک در یک میلیون مثبت کاذب(خطا) به دام می‌اندازد. بااستفاده از SMG ، سازمان ها می‌توانند به طور موثر تهدیدهای جدید پیام رسانی را خنثی کرده، اختلال در شبکه را به حداقل رسانده و بهره وری کارمندان و اعتبار شرکت/سازمان را حفظ کنند.

SMG از بروزرسانی های خودکار بلادرنگ آنتی اسپم و ضد بدافزار شبکه Global Intelligence Network ™ سیمانتک، فناوری حفاظت از حمله هدفمند خلع قدرت سیمانتک (Disarm targeted attack protection technology)، قوانین خاص مشتری و on-box connection throttling استفاده می‌کند.

گزارش دهی جامع به مدیران شبکه، این امکان را می‌دهد تا بر وضعیت کلی امنیتی سازمان متمرکز شده و در عین حال وضعیت را به مدیران کلیدی گزارش دهند .فیلتر پیشرفته محتوا ، DLP و رمزگذاری ایمیل به سازمان ها کمک می‌کند تا داده های حساس را کنترل کنند ، خطرات و هزینه های مربوط به از دست دادن داده ها را کاهش داده و همزمان خواسته های مربوط به مقررات و حاکمیت شرکتی را برآورده کنند.

SMG به صورت یک دستگاه فیزیکی و یا یک ماشین مجازی VMware یا Microsoft Hyper-V در دسترس است که به سازمان / شرکتها این امکان را می‌دهد تا به راحتی بتوانند امنیت ایمیل خود را پیاده سازی کنند.



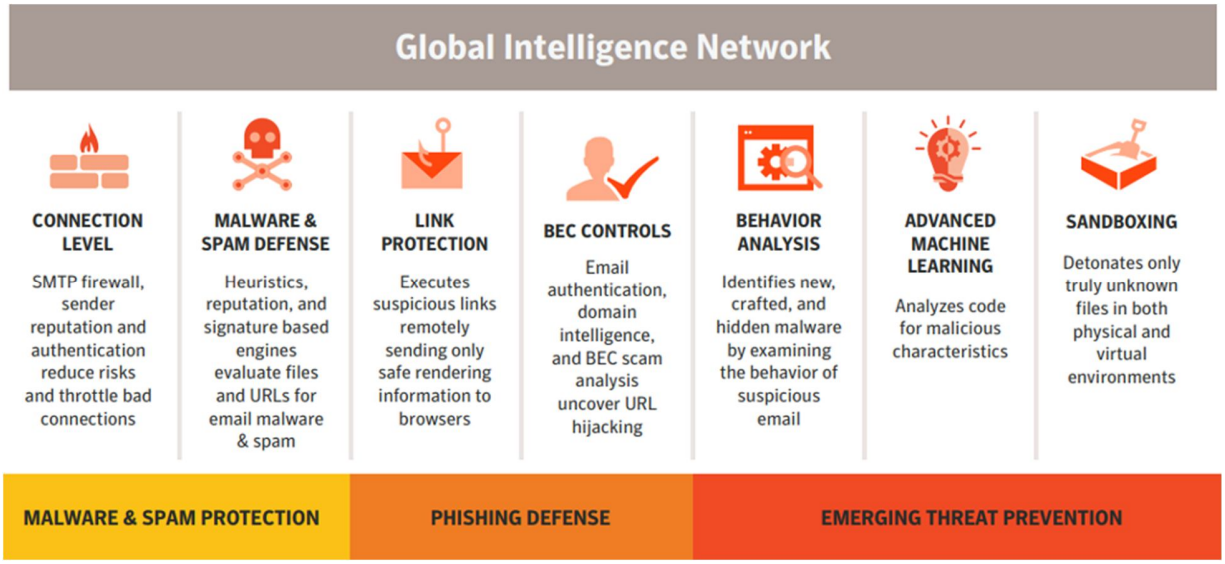
کاهش قرارگیری در معرض خطر

بهترین محافظت با کارآیی برتر و شناسایی تهدیدات شخصی سازی شده

دروازه پیام رسانی توسط موتور آنتی اسپم Symantec Brightmail تأمین می‌شود - مجموعه ای از فناوری ها که تهدیدات ناشی از ایمیل را براساس اعتبار در سطح جهانی و محلی شناسایی می‌کنند .این فناوری، این امکان را برای شما فراهم می‌کند تا بیش از ۹۹ درصد اسپم ها را با کمتر از یک در یک میلیون مثبت کاذب مسدود کرده و علاوه بر این تا ۹۰ درصد ایمیل های ناخواسته را قبل از دسترسی به شبکه شما مسدود کند.

راه حل های امنیتی پیام رسان سیمانتک که توسط یکی از بزرگترین سازمان های تحقیقاتی بدافزار جهان، یعنی شبکه اطلاعاتی جهانی سیمانتک(Symantec Global Intelligence Network) پشتیبانی می‌شود ، با بهره گیری از اطلاعات بی درنگ، از ۱۲۰ میلیون دستگاه و بیش از ۸۵ میلیون کاربر ، برای شناسایی تهدیدهای جدید استفاده می‌کند.

بخش کلیدی شبکه اطلاعات جهانی سیمانتک، شبکه Symantec Probe است – سیستمی‌متشکل از بالغ بر پنج میلیون حساب ایمیل و دامنه تله مانند، بر جمع آوری نمونه های کلاهبرداری ، فیشینگ و اسپم. شبکه پروب حضور جهانی دارد ، از جمله استقرار هدفمند برای محتوای زبان خارجی و اندازه گیری فعالیت های اسپم و فیشینگ جهانی. سیمانتک هر روز بیش از سه میلیارد پیام ایمیل را تجزیه و تحلیل می‌کند و بیش از ۸۵۰ میلیون صندوق پستی را در برابر تهدیدات اسپم و بدافزار محافظت می‌کند .همچنین داده های اعتبار URL برای جلوگیری از اسپم ، بدافزار و پیام های فیشینگ با شناسایی URLهای تهدید موجود در پیام ها ، جمع آوری می‌شود.

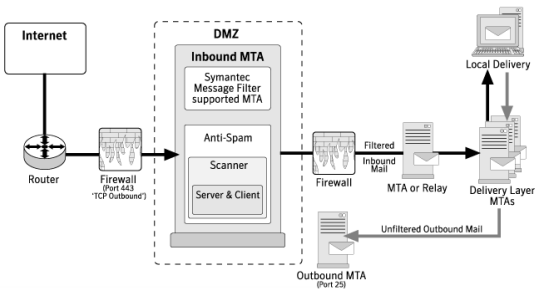


فناوری Symantec Disarm (خلع سلاح) با حذف تهدیدات روز صفر مرتبط با اسناد از پیوست های Microsoft Office و PDF، کاربران را در برابر حملات هدفمند محافظت می‌کند . محتوای فعال احتمالی مخرب از پیوست حذف شده و سند پس از پاکسازی، بازسازی شده و دوباره به ایمیل متصل شده و به مقصد ارسال می‌شود .خلع سلاح ، تهدیدهای دیده نشده و شناخته شده را متوقف می‌کند.

قوانین خاص مشتری این امکان را برای مشتریان فراهم می‌کند که علاوه بر قوانین آنتی اسپم سیمانتک ، قوانین اسپم شخصی را نیز بدست آورند.

این امر کاملاً براساس موارد ارسالی از طرف مدیران و کاربران نهایی ، با کنترل کامل بر تهاجمی‌بودن ایجاد فیلتر و توانایی حذف فوری قوانین متناسب با آنها - در صورت مثبت بودن کاذب - است.

کاربران می‌توانند پیام ها را به سیمانتک ارسال کنند و براساس تنظیمات مدیر، رولها و فیلترهای جدیدی ایجاد می‌شود. رولهای خاص مشتری، محافظت خودکار در برابر حملات ناخواسته و اسپم های نوظهور را ارائه می‌دهد .از همه مهمتر ، این امر می‌تواند به جلوگیری از حملات ایمیل که مستقیماً شرکت/سازمان شما و کاربران نهایی را هدف قرار می‌دهد ، کمک کند.

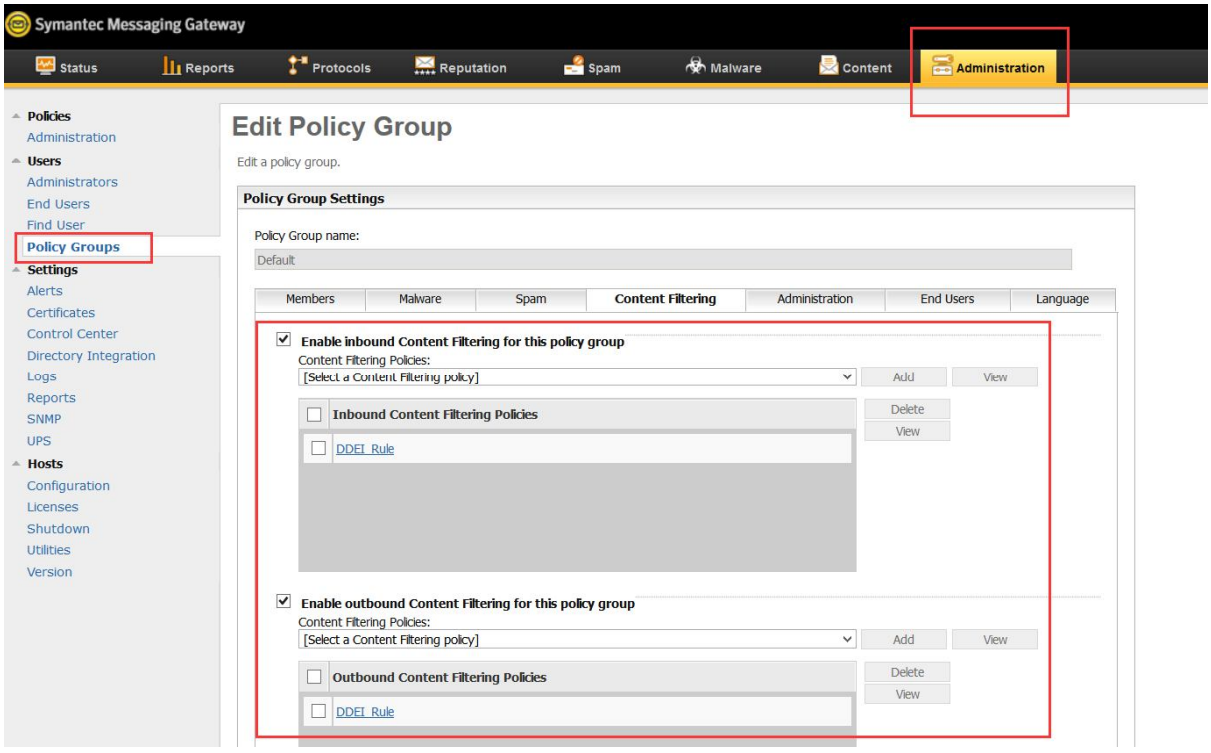


کنترل بیشتر با جلوگیری از نشت داده ها و رمزگذاری ایمیل

نشت اطلاعات حساس شرکت/سازمان شما می‌تواند منجر به آسیب زدن به اعتبار شرکت/سازمان، از دست دادن مشتریان و در نهایت کاهش درآمد شود – شکستی که هیچ شرکت یا سازمانی از عهده آن برنمی‌آید. SMG دارای فن آوری پیشرفته فیلتر کردن محتوا و DLP است که محافظت و کنترل داده های حساس را آسان می‌کند. مدیران می‌توانند به راحتی سیاست های موثر و انعطاف پذیر ایجاد کنند که تطابق رولها را اعمال می‌کند و از نشت داده ها محافظت می‌کند .دستگاه های SMG از فناوری پیشرفته تطبیق داده ساختاری Symantec DLP، که داده های نگهداری شده در پایگاه داده های شما ، مانند سوابق مشتری و بیمار ، اطلاعات بانکی ، پردازش سفارش یا مدیریت ارتباط با مشتری (CRM) را تجزیه و تحلیل می‌کند و اثر انگشت منحصر به فردی برای داده های واقعی ایجاد می‌کند، استفاده می‌کند.

علاوه بر قابلیت های جلوگیری از از نشت داده های جعبه ای ، SMG این توانایی را دارد که به عنوان یک نقطه اجرای محصول Symantec DLP عمل کرده و به شما امکان نظارت و محافظت از اطلاعات حساس ارسالی از طریق ایمیل را بدهد و همجنین از پایان یافتن اطلاعات در جایی که به آن تعلق دارد اطمینان بدهد. قابلیت مدیریت قرنطینه یکپارچه به مدیران این امکان را می‌دهد تا از طریق کنسول Symantec Data Loss Prevention Enforce، مواردی که توسط SMG قرنطینه شده اند را به طور مستقیم مدیریت و اقدام کنند. برای امنیت بیشتر ، هنگام ارسال پیام به Symantec Data Loss Prevention از رمزگذاری Transport Layer Security (TLS)استفاده می‌شود.

SMG افزونه رمزگذاری محتوای سیمانتک را ارائه می‌دهد که می‌تواند به عنوان سرویس میزبانی شده (hosted) و یا به صورت نصب در محل (on-premise) ارایه شود. برای مشتریانی که رمزگذاری میزبانی شده را ترجیح می‌دهند ، رمزگذاری محتوای Symantec که توسط Symantec.cloud



ارائه شده است ، رمزگذاری خودکار را بر اساس سیاست ها ارائه می‌دهد و گزینه های انعطاف پذیر ارسال پیام را فراهم کرده و دریافت و پاسخ ایمن برای گیرندگان را آسان می‌کند .برای مشتریانی که رمزگذاری نصب در سرور محلی را ترجیح می‌دهند ، SMG می‌تواند با Symantec Gateway Email Encryption طراحی شده توسط PGP Technology تلفیق شود .به عنوان نقطه اجرای سیاست ، SMG پیام ها را بر اساس معیارهای تعیین شده توسط مشتری ارزیابی می‌کند و در صورت تشخیص رمزگذاری ضروری ، آنها را به Gateway Email Encryption می‌فرستد تا براساس خط مشی های مشخص شده توسط مشتری، رمزگذاری شود.

از آنجا که امروزه رایج ترین شکل ارتباطات تجاری از طریق ایمیل می‌باشد، تعداد بیشتری از شرکت/سازمان ها ابه لزوم رمزگذاری ایمیل پی برده اند.

.با ترکیب قابلیت فیلتر کردن محتوا و DLP در SMG که هر دو توسط یک شرکت واحد یعنی سیمانتک ارایه می‌شود، هزینه های کلی کاهش یافته و مدیریت آسان گشته است.

کاهش هزینه و پیچیدگی با مدیریت آسان

انعطاف پذیری و انتخاب

محیط IT شما منحصر به فرد و متناسب با نیازهای کاری شماست .ترجیحات و الزامات شما برای استقرار یک فناوری امنیتی پیام رسانی می‌تواند در سازمان های دیگر بسیار متفاوت باشد .با ارائه گزینه های استقرار انعطاف پذیر ، SMG متناسب با نیازهای خاص شما تنظیم می‌شود .علاوه بر استقرار SMG در یک دستگاه سخت افزاری فیزیکی ، شما این امکان را دارید که آن را در ماشین مجازی مستقر کنید . SMG با هر دو محیط مجازی VMware و Microsoft Hyper-V سازگار است.

قابلیت پشتیبانی IPv6 به این معنی است که می‌توانید Gatewayپیام رسانی خود را در یک شبکه مخلوط / IPv4مستقر کنید .این امکان را برای مشتریان فراهم می‌کند تا ترافیک ایمیل مبتنی بر IPv6 را پردازش ، اسکن و گزارش کنند.

مدیریت و راهبری واحد

SMG شامل یک مرکز کنترل قدرتمند برای مدیریت واحد و مدیریت زیرساخت پیام رسانی شرکت/سازمان شما است .از یک کنسول مبتنی بر وب ، مدیران می‌توانند به راحتی چندین دستگاه SMG را برای مشاهده روندها ، آمار حمله و حوادث عدم انطباق مدیریت کنند .از LDAP می‌توان برای تأیید اعتبار دسترسی اداری و پیکربندی گروه ها و خط مشی ها استفاده کرد .با از بین بردن پیچیدگی چندین کنسول ، سیاست های متفاوت و روش های ناسازگار گزارشگیری و لاگ (log) ، SMG به طور قابل توجهی هزینه کل مالکیت زیرساخت های امنیت پیام رسانی را کاهش می‌دهد.

SMG از مجموعه کاملی از گزینه های گزارش دهی پشتیبانی می‌کند ، از جمله داشبورد و خلاصه های اجرایی که اثر بخشی و تأثیر سیستم را برجسته می‌کند. گزارش دهی به مدیران کمک می‌کند تا به طور فعالانه روند از دست دادن داده ها را شناسایی و انطباق را شرح دهند. کنسول مدیریت شامل بیش از ۵۰ گزارش از پیش تعیین شده است که می‌تواند براساس محتوا یا زمان تنظیم شود ، برای تولید گزارش خودکار برنامه ریزی شده و صادر شود.

ردیابی ساده پیام از طریق یک رابط گرافیکی حسابرسی پیام، به مدیران این امکان را می‌دهد تا به سرعت وضعیت پیام و وضعیت تحویل پیام را تعیین کنند

بازخورد ارسالی برای قوانین خاص مشتری در دسترس است و این کار به مدیران اجازه می‌دهد نسبت به آنچه کاربران ارسال می‌کنند و آیا رولی برای پیام ارسالی وجود دارد، یک دیدی داشته باشند.

با افزایش هرزنامه ها ، SMG این امکان را برای مدیران فراهم می‌کند که تعریف خود را از ایمیل ناخواسته با ایجاد سیاست هایی برای خبرنامه ها و ایمیل های بازاریابی شخصی سازی کنند.

SMG به تنظیمات کمی‌خارج از جعبه احتیاج دارد که استقرار اولیه را آسان و سریع می‌کند. امضای هرزنامه و تعاریف بدافزار به طور خودکار در زمان واقعی به روز می‌شوند و از شبکه قدرتمند Global Intelligence استفاده می‌کند تا مدیریت را ساده کرده و از مزایای جدیدترین تشخیص تهدید در شرکت/سازمان شما اطمینان حاصل کند.

مزایای اصلی

- بیش از ۹۹ درصد هرزنامه را با کمتر از یک در یک میلیون مثبت کاذب و به روزرسانی خودکار در زمان واقعی مسدود می‌کند.
- محافظت در برابر حمله هدفمند ، بدافزار و تهدیدات روز صفر.
- قوانین خاص مشتری به مشتریان اجازه می‌دهد تا مجموعه قوانین متناسب با محیط خاص خود را با گزارش دهی آسان برای تعیین اثربخشی قوانین سفارشی ایجاد کنند.
- با استفاده از قابلیت اثر انگشت و شناسایی داده های واقعی شرکت/سازمان در پیام ها یا پیوست ها ، از نشت اطلاعات حساس مشتری و اطلاعات محرمانه با ارزش محافظت می‌کند.
- از اعتبار شرکت/سازمان محافظت می‌کند و خطرات مرتبط با نشت داده ها ، حاکمیت داخلی و انطباق با مقررات را مدیریت می‌کند.
- پردازش ، اسکن و گزارش در مورد ترافیک ایمیل با پروتکل IPv6
- اشتراک اختیاری Symantec Content Encryption رمزگذاری ایمیل را در کنسول SMG ادغام کرده و از سیاست های قدرتمند فیلتر محتوا و DLP استفاده می‌کند.
- شامل داشبورد ، گزارش های خلاصه و گزارش های دقیق نشان دهنده کارایی و تأثیر SMG در حالی که به طور فعال روندهای تهدید و موارد بالقوه انطباق را برجسته می‌کند.
- با حذف پیچیدگی چندین کنسول ، سیاست های پراکنده و ثبت و گزارش ناسازگار، ضمن اثبات کارایی و تأثیر امنیت پیام رسانی، هزینه های مدیریتی کاهش می‌یابد.
- Global Intelligence Network به روزرسانی های بی درنگ محافظت از اسپم و بدافزار برای بالغ بر ۸۵۰ میلیون صندوق پستی محافظت شده و بیش از پنج میلیون حساب در شبکه Probe سیمانتک، ارائه می‌دهد.
- پیش از ایجاد اختلال، از تهدیدهای جدید و در حال ظهور، محافظت می‌کند.
- SMG به دو صورت سخت افزاری و ماشین مجازی ارایه می‌شود.

نیازمندیهای سیستم

پلتفرم های پشتیبانی شده

SMG را می‌توان در خانواده ای از تجهیزات سخت افزاری سری Symantec 8300 مستقر کرد که می‌تواند در سازمان ها از مشاغل کوچک تا شرکت های بزرگ مقیاس بندی شود. یک گزینه تجهیز مجازی نیز وجود دارد ، SMG نسخه مجازی ، که همان نرم افزار ، ویژگی ها و عملکردهای مختلف را در محیط های VMware یا Microsoft Hyper-V مستقر می‌کند. تجهیزات می‌توانند به عنوان مراکز کنترل اختصاصی ، اسکنرها ، یا مرکز کنترل / اسکنرهای ترکیبی مستقر شوند.

الزامات مرورگر (کنسول مدیریتی)

- Microsoft Internet Explorer 9، 10 یا 11
- Mozilla Firefox 28 یا بالاتر
- Google Chrome 34 یا بالاتر

پلتفرم سخت افزاری

- تجهیزات Symantec SMG سری ۸۳۰۰
- تجهیزات Brightmail سیمانتک سری ۸۳۰۰

هایپروایزورهای مجازی (نسخه مجازی)

- VMware ESXi/ESX/vSphere 5.x, 6.x
- Microsoft Hyper-V 2008 به بالا

اطلاعات بیشتر:

http://www.symantec.com/messaging-gateway

Appliance Model	8340	8380
Organization	Small and Medium Businesses	Enterprise/Large Enterprise
Typical Deployment*	Control Center/Scanner	Dedicated Scanner or Control Center
Form Factor	1RU Rack Mount	1RU Rack Mount
Power Supply	Single	Redundant, hot-plug, auto-switching, universal power supply
CPU	Single Quad-Core Processor	Dual 6-Core Processors
Hard Drive / RAID	2 x 1TB SAS RAID 1	6 x 300GB Serial-Attach SCSI (hot-swappable) RAID 10
NIC	Two Gigabit Ethernet Ports	Four Gigabit Ethernet Ports
** Customers may deploy any appliance model as a combined control center/scanner, dedicated scanner, or dedicated control center*		

درباه سیمانتک: شرکت سیمانتک، در سال ۱۹۸۲ تاسیس شده و با بیش از ۱۹۰۰۰ کارمند، یکی از غول های فناوری اطلاعات و امنیت اطلاعات در جهان است. ۹۹٪ از شرکت های فورچون ۵۰۰ (بزرگترین شرکت های جهان) از محصولات سیمانتک استفاده می‌کنند.

رایان سامانه آرکا- نماینده رسمی سیمانتک در ایران

تهران، خیابان شهید بهشتی ، خیابان پاکستان ، کوچه چهارم ، پلاک ۱۱ ، طبقه چهارم ، واحد ۷
تلفن: ۸۸۸۰۴۹۶۱ | دورنگار: ۸۹۷۸۳۷۳۷ | کدپستی : ۱۵۳۱۶۴۵۹۱۸
info@arka.ir www.arka.ir

کلیه حقوق مادی و معنوی محفوظ و متعلق به شرکت رایان سامانه آرکا می‌باشد.