DATA SHEET

Messaging Gateway On-Premises Appliance

❖ مقدمه

امنیت ایمیل جامع و هوشمند، چه سیستم ایمیل شما درون سازمانی باشد، چه مبتنی بر فضای ابری یا هر دو، با درکی شفاف و واقعی از آنچه قصد مبارزه با آن را دارید شروع می شود. ایمیل هنوز محبوب ترین و فراگیرترین ابزاری است که مجرمان سایبری برای ایجاد و توزیع تهدیدها از جمله spear phishing، باج افزارها و رخنه در ایمیل های سازمانی (business email compromise) از آن استفاده می کنند. بر اساس گزارش تهدید امنیت اینترنتی (ISTR) سیمانتک ۲۰۱۸، در سال ۲۰۱۷ از هر ۴۱۲ ایمیل یک ایمیل حاوی حمله بدافزار بوده است، هر ماه ۷،۷۱۰ سازمان هدف رخنه در ایمیل های سازمانی قرار گرفته و spear phishing پرکاربردترین ابزار انتشار ویروس است که توسط ۷۱ درصد گروه های حملات هدفمند استفاده می شود.

❖ معرفی محصول Messaging Gateway

Messaging Gateway شرکت Symantec یک راه حل امنیت ایمیلی درون سازمانی است که امنیت پیام رسانی ورودی و خروجی از جمله محافظت قدرتمند دربرابر آخرین تهدیدهای پیام ر سانی، مثل باج افزارها، spear phishing و رخنه در ایمیل های سازمانی را فراهم می کند. این محصول بیش از ۹۹ درصد هرزنامه ها (spam) را با کمتر از ۱خطای مثبت در هر ۱ میلیون به دام انداخته و با دریافت بلادرنگ اطلاعات ضدهرزنامه و ضدبدافزار از Symantec Global Intelegence Network پاسخ موثری به تهدیدهای جدید و ناشناخته در قالب ایمیل ها می دهد، همچنین قابلیت های حفاظت از داده ها (DLP)، ایمیل های کاربران را ایمن و محرمانه نگاه می دارد.

Messaging Gateway را می توان به صورت ابزار مجازی یا فیزیکی پیاده سازی کرد و شما می توانید هنگام افزایش حجم هرزنامه ها، برای حفظ جریان پیام ها به سادگی ظرفیت را اضافه کنید.

❖ **توقف تهدیدهای پیشرفته در مسیر آنها**

Messaging Gateway فن آوری های شـــناســـایی چندلایه را با اطلاعات موجود در بزرگترین بانک اطلاعات تهدیدات غیرنظامی دنیا (Symantec Global Intelegence Network) برای م سدود سازی و قرنطینه سازی موثر ایمل های مخرب ترکیب می کند.

فیلترینگ چندلایه هرزنامه و بدافزار:

مسدودسازی ایمیل های ناخواسته و پیشگیری از تحویل لینک ها و پیوست های مخرب.

محافظت دربرابر حملات هدفمند:

محافظت قدرتمند در برابر spear phishing ، باج افزار و رخنه در ایمیل های سازمانی.

فیلترینگ محتوا و پیشگیری از مفقود شدن داده:

فیلتر محتوا برای دفاع موثر در برابر نفوذ و پیشگیری از نشت اطلاعات حساس شرکت.

- توقف حملات BEC با اســتفاده از فناوری heuristics پیشــرفته، موتور تحلیل کلاهبرداری BEC، احراز هویت فرستنده و اطلاعات دامنه برای توقف سرقت URL و جعل هویت.
- Symantec Email Fraud Protection ساخت پروتکل های احراز هویت فرستنده (DMARC, DKIM, SPF) را اتوماتیک می کند،تا همه گیرنده ها از حملات جعل هویت مصون بمانند.
- دفاع در برابر لینک های مخربی که در کمپین های spear phishing به کار می رود با فیلترینگ اعتبار URL برا ساس پایگاه داده جهانی سیمانتک که شنا سایی متنوع و پی شرفته فی شینگ را در بر می گیرد، و لینک های spear phishing را پیدا می کند که شبیه حملات فیشینگ شناخته شده هستند.
- محافظت از کاربران دربرابر حملات هدفمند مثل باج افزارها، با حذف تهدیدات روز صفر از فایل های مایکرو سافت آفیس و پیوســت های PDF. محتوای فعال و به طور بالقوه مخرب یک فایل پیوســت حذف شــده و ســندی تمیز مجددا ساخته شده، دوباره به ایمیل پیوست شده و به کاربر نهایی ارسال می شود.
- مسدودسازی هرزنامه ها و حملات directory harvesting با استفاده از ترکیب پایگاه های داده Symantec و درون سازمانی جهت اعتبار سنجی فر ستنده، تعریف قوانین سفار شی ضد هرزنامه ها در کنار فناوری heuristics مورد ا ستفاده تا ۹۹ در صد ایمیل های ناخوا سته را قبل از ر سیدن به شبکه شما م سدود می کند. محدود کردن

ایمیل های ارسالی مانع حملات اسپم از جانب کاربران پرخطر داخلی و کاهش اعتبار سرور ایمیل سازمان در اینترنت می شود.

- دفاع دربرابر لینک های مخربی که در کمپین های spear phishing استفاده می شود با فیلترینگ اعتبار URL برا ساس پایگاه جهانی سیمانتک (Symantec Global Intelegence Network) که شنا سایی فی شینگ پیشرفته را شامل شده و لینک های spear phishing را پیدا می کند که شبیه حملات فیشینگ شناخته شده هستند.

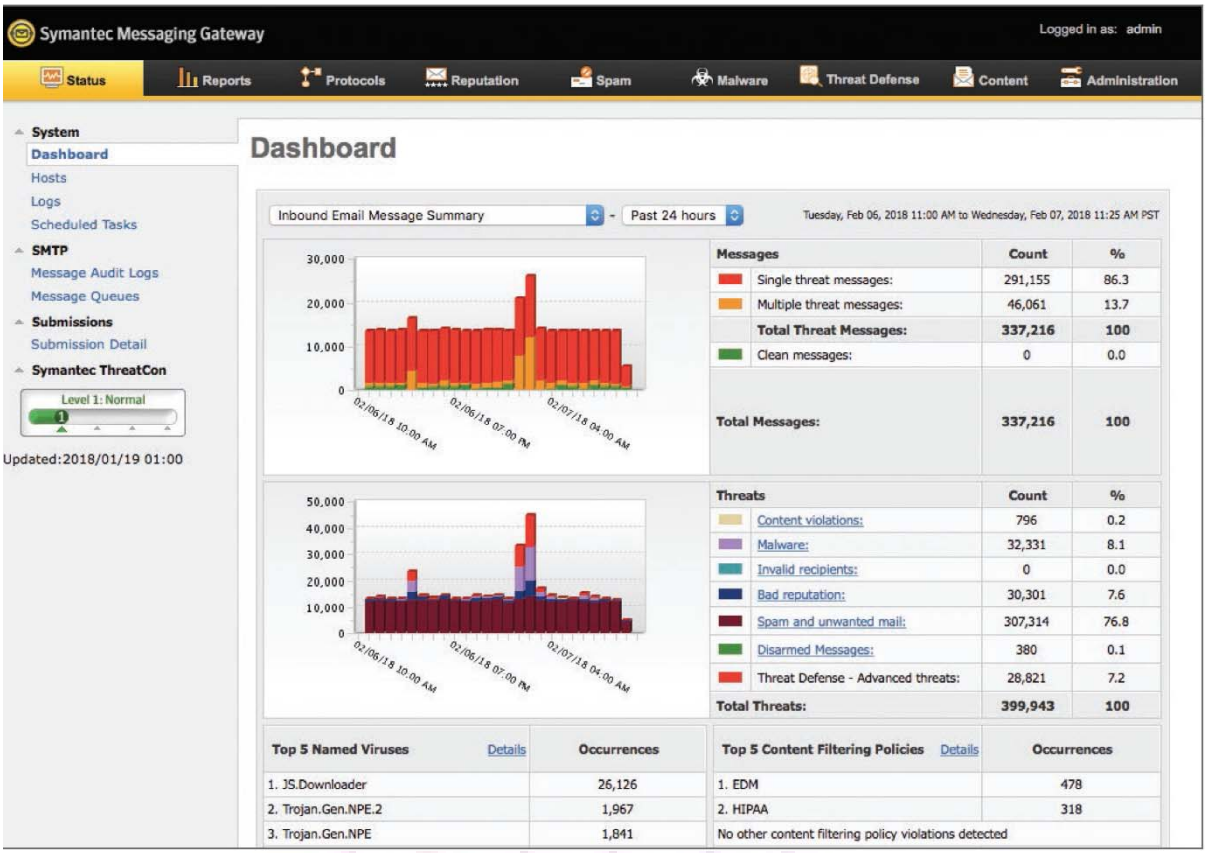
❖ **محافظت از داده های حساس؛ پیشگیری از ایمیل ناخواسته**

Messaging Gateway فیلترینگ محتوای داخلی و کنترل هایی برای پیشگیری از نشت داده ها ارائه می دهد که ایمیل های حساس و ناخواسته را مسدود یا قرنطینه می کند.

- کنترل های پیشرفتهٔ محافظت از محتوا مانع دریافت ایمیل های ناخواسته (مثل خبرنامه ها و دیگر محتواهای بازاریابی) از طرف کاربران می گردد.
- قابلیت پیشگیری از نشت اطلاعات (DLP)، حفاظت از داده های سازمان در درون پیام ها یا پیوست ها را ساده تر می نماید. شما می توانید با استفاده از ۱۰۰ قالب، الگو و فهرست از پیش ساخته شده سیاست های موثر و انعطاف پذیری را تدوین کنید که در پیاده سازی سیاست های سازمان در حفاظت و جلوگیری از نشت اطلاعات به شما کمک می نماید.
- رمزگذاری TLS پروتکل SMTP به صورت خودکار به شما تضمین می دهد همه ارتباطات ایمیلی در حال مخابره، امن هستند.

❖ **مدیریت امنیت پیام رسانی با قابلیت دید زیاد:**

یک کنسول مبتنی بر وب پیکربندی و کنترل مجزا، گزارش مفصل، و یک چشم انداز منسجم از روند تهدیدها، آمار حملات و رویدادهای عدم انطباق را ارائه می دهد. چند نسخه Messaging Gateway را می توان در یک محیط ترکیبی IPv4/IPv6 مدیریت کرد.



- گزارش های دقیق، خلاصه و جامع از جمله ۵۰ گزارش کنونی که توسط محتوا و زمانبندی قابل سفارشی سازی بوده و بر روند تهدیدها و مشکلات بالقوه انطباق تاکید می کنند.
- داده های تولیدی Syslog را می توان برای تحلیل همبستگی بیشتر به ابزارهای اطلاعات و امنیت شخص ثالث (SIEM) منتقل کرد.
- ردیابی ساده پیام با استفاده از واسطه تصویری بازبینی پیام که امکان تعیین سریع وضعیت پیام و وضعیت تحویل آن را فراهم می کند.
- دریافت خودکار هشدارها و اعلان تهدیدها درباره شیوع ویروس، نقض سیاست و اطلاعات قرنطینه.

❖ ادغام با Symantec DLP ، Threat Isolation ، Content Analysis

- برای قابلیت های بیشتر و پیشرفته تر محافظت دربرابر تهدیدها، Messaging Gateway می تواند محتوای مبتنی بر فایل پیام رسانی را برای بازبینی بیشتر به Symantec Content Analysis منتقل کند. این کار شامل هوش عملی می شود که تحلیل ایستا، یادگیری ماشینی و تکنیک های تحلیل رفتار را ترکیب می کند. یک

جعبه شنی سازگار و قابل سفارشی سازی، انفجار جامع بدافزارها را برای تحلیل سریع فایل های مشکوک، تعامل با بدافزار درحال اجرا برای افشای رفتار کامل آن، و افشای تهدیدهای روز صفر و بدافزارهای ناشناخته ارائه می دهد.

- برای محافظت پیشـــرفته در مقابل لینک های مخرب وب که در ایمیل قرار می گیرند، URL ها را می توان در Symantec Email Threat Isolation بازنویسی کرد، یک فن آوری که نشست های وب را خارج از سیستم مقصد اجرا می کند. ارسال اطلاعات رندرینگ ایمن به کاربران مانع رسیدن بدافزارهای روز صفر وب سایت ها به دستگاه های کاربران می شود. قراردادن سایت های اسپیر فیشینگ بالقوه در وضعیت فقط خواندنی نیز سرقت مدارک را متوقف می کند، چون کاربران از ارسال اطلاعات محرمانه شرکت یا دیگر اطلاعات حساس منع شده اند.
- برای سازمان هایی که از راه حل DLP سیمانتک استفاده می کنند یا آنها که قصد استفاده از این راه حل پیشرو در بازار را دارند، Messaging Gateway به خوبی به DLP ادغام شده تا سیاست تقویت به کانال ایمیل بسط یابد. رمزگذاری مبتنی بر سیاست به صورت افزونه Symantec Content Encryption در دسترس است.

❖ گواهی نامه های دریافت شده توسط محصول Messaging Gateway

- Common Crieria EAL2
- FIPS 140-2

❖ سیستم مورد نیاز:

ابزار مجازی (ویژگی ها و کارکرد یکسان)

- VMware ESXI™/VMware ESX®, VMware vSphere® 5.x, 6.x
- Microsoft Hyper-V® 2008 or 2012

مرورگرها (برای کنسول اجرایی)

- Microsoft Internet Explorer® 11.0 یا بالاتر
- Mozilla® Firefox® 45 یا بالاتر
- Google Chrome™ 55 یا بالاتر