Trellix

Trellix MOVE AntiVirus

امنیت برای بستر مجازی سازمان، با کارایی بسیار بالا

نرم‌افزارهای ضدویروس سنتی عملکرد مناسب و قابل قبولی در بسترهای مجازی ندارند. Trellix Management for Optimized Virtual Environments AntiVirus – به اختصار Trellix MOVE AV – محافظت جامع و بهینه‌شده‌ای را برای ماشین‌ها و سرورهای مجازی فراهم می‌آورد. قابل پیاده‌سازی بر روی چندین نوع بستر مجازی مختلف و یا بکارگیری آن بدون نیاز به "سفیر" (Agent) در محیط‌های مبتنی بر VMware NSX. صرف‌نظر از هر روش راه‌اندازی، امنیتی کارآمد را بدون اثرگذاری منفی بر روی کارایی ماشین‌های مجازی در اختیار خواهید داشت.

پویش بهینه‌شده

ماهیت دائماً در حال تغییر ماشین‌ها و سرورهای مجازی، نیاز به مدیریت اجرایی دقیق دارد. در حالت خاموش (Offline)، تمام ماشین‌های مجازی باید سالم و عاری از بدافزار باشند و یا به محض درخواست یک کاربر برای شروع به کار، بدون تأخیر کنترل شوند. ضدویروس تنها سرویسی نخواهد بود که باید اجرا و راه‌اندازی شود و اغلب، کاربران به‌صورت گروهی شروع به کار می‌کنند. در این وضعیت، درخواست برای ضدویروس به اوج می‌رسد و می‌تواند حالت "طوفان ضدویروس" (AntiVirus Storm) را ایجاد کند. حالتی که ضدویروس تمام منابع را مصرف کرده و امکان شروع به کار را از کاربر می‌گیرد. برای جلوگیری از ایجاد گلوگاه و تأخیر در اجرای سیاست‌ها، Trellix MOVE AV برخی از امور خود را از تک‌تک ماشین‌های مجازی کاربران به یک ماشین مجازی اختصاصی و مقاوم‌شده با عنوان Security Virtual Machine – به اختصار SVM –، انتقال می‌دهد. عملیاتی نظیر پویش (Scan)، اعمال تنظیمات و به‌روزرسانی بر روی ماشین مجازی اختصاصی انجام می‌شود. محصول Trellix MOVE AV یک انباره بزرگ و فراگیر از فایل‌های کنترل‌شده و سالم را تهیه و نگهداری می‌کند تا هر بار که یک ماشین مجازی درخواست دسترسی به این فایل‌ها را دارد، نیازی به صبر کردن و کنترل مجدد توسط ضدویروس نباشد. در نتیجه، حافظه اختصاص داده شده به هر ماشین مجازی کاهش یافته و حافظه آزادشده می‌تواند در محل‌های دیگر به کار گرفته شود.

مدیریت مرکزی

کنسول نام آشنای Trellix ePolicy Orchestrator – به اختصار Trellix ePO – شما را قادر به پیکربندی متمرکز تنظیمات و کنترل‌های Trellix MOVE AV می‌کند. در این کنسول، وضعیت امنیتی دستگاه‌های فیزیکی در کنار ماشین‌های مجازی، قابل رصد است. با رویکرد مدرن و پیشرفته Trellix MOVE AV، راهبران قادرند تا از طریق این کنسول قدرتمند و با بهره‌گیری از Trellix Cloud Workload Discovery یک سیاست را به یک ماشین مجازی، به یک Cluster یا به سرتاسر مرکز داده اعمال کنند.

قابلیت‌های کلیدی

- **تقسیم بار پویش**
  حفاظت فوری با اثرگذاری اندک بر روی حافظه و پردازشگر
- **جلوگیری از طوفان ضدویروس**
  تنظیمات متنوع برای پویش‌های بلادرنگ و در زمان نیاز
- **توزیع منعطف**
  پیاده‌سازی Multiplatform، قابل اجرا بر روی تمامی بسترهای مجازی‌سازی یا پیاده‌سازی Agentless در بسترهای VMware NSX
- **مسدودسازی تهدیدات روز صفر و ناشناخته**
  تحلیل فایل‌های ناشناخته و مشکوک با بررسی پیشینه آنها و بهره‌گیری از فناوری‌های رفتارشناسی در یک محیط قرنطینه امن (قابل اجرا در حالت Multiplatform در صورت استفاده از راهکار مربوطه)
- **مدیریت یکپارچه و گزارش‌های متنوع**
  مدیریت متمرکز و جامع دستگاه‌های فیزیکی، ماشین‌های مجازی و بسترهای ابری سازمان از طریق کنسول مدیریتی قدرتمند Trellix ePO

معماری Agentless

در این معماری، Trellix MOVE AV با بهره‌گیری از VMware NSX اثربخشی بالایی را در این بسترها فراهم می‌سازد. بدین صورت که از Hypervisor به‌عنوان یک ارتباط با سرعت بالا که امکان پویش شدن ماشین‌های مجازی توسط SVM را در خارج از ماشین فراهم می‌کند استفاده می‌شود. با انجام پویش توسط SVM، ثبت شدن فایل پاک – برای جلوگیری از پویش شدن مجدد آن – و همچنین حذف، مسدودسازی دسترسی و یا قرنطینه نمودن فایل‌های مخرب به VMware NSXi محول می‌شود. پس از نصب و پیکربندی SVM و VMware NSX بر روی سرورهای VMware ESXi، ماشین‌ها بدون نیاز به نصب هر گونه نرم‌افزار ترلیکس بر روی آنها به‌صورت خودکار تحت حفاظت قرار می‌گیرند. همچنین با پیاده‌سازی Trellix MOVE AV در حالت موسوم به vMotion-aware، انتقال ماشین‌های مجازی از یک دستگاه میزبان (Host) به دستگاه میزبان دیگر بدون تأثیر بر روی پویش‌ها و فعالیت کاربر قابل انجام خواهد بود.

معماری Multiplatform

در معماری Multiplatform با پشتیبانی از تمامی بسترهای مجازی‌سازی رایج از جمله vSphere، Hyper-V، KVM و XenServer، سفیر Trellix MOVE AV نصب شده بر روی ماشین مجازی، با برقراری ارتباط با SVM، بخش قابل توجهی از بار پویش و پردازش‌های شناسایی را به آن منتقل می‌کند. سفیر Trellix MOVE AV از یک حافظه نهان محلی (Local Cache) بهره‌گیری کرده و سیاست‌ها و توابع پویش را مدیریت می‌کند. همچنین در این معماری می‌توان با پویش یک Image از ماشین مجازی، از آن به‌عنوان نمونه اصلی در ساخت ماشین‌های مجازی دیگر استفاده کرد. وجود حافظه نهان محلی در این نمونه اصلی، سبب بالا آمدن سریع‌تر ماشین‌های مجازی ساخته شده بر اساس آن خواهد شد. به‌محض دسترسی فایل بر روی یک ماشین مجازی، ماشین پویشگر Offload بطور بلادرنگ آن را بررسی کرده و پاسخ مناسب را به ماشین باز می‌گرداند. در این معماری این امکان نیز فراهم است که کاربر از طریق هشدارهای نمایش داده شده از وضعیت آلودگی فایل آگاه شود. در حالت Multiplatform، با بالا و پایین شدن درخواست‌های پویش، ماشین‌های SVM به‌صورت خودکار منابع خود را افزایش و کاهش می‌دهند تا اثربخشی بیشتری را برای بستر مجازی‌سازی فراهم کنند. Trellix MOVE AV با بهره‌گیری از Trellix Global Threat Intelligence – به اختصار Trellix GTI – و داده‌های جمع‌آوری‌شده در شبکه محلی از طریق Trellix Threat Intelligence Exchange که بطور جداگانه عرضه می‌شود قادر به شناسایی جدیدترین و ناشناخته‌ترین تهدیدات و مقابله با آنها خواهد بود.

مزایای کلیدی

مدیریت و دید گسترده

- افزایش دقت پویش‌ها با انجام هدفمند پویش‌های در زمان نیاز
- توزیع خودکار SVM بر روی هر Hypervisor با بهره‌گیری از NSX Service Composer
- آگاهی از رویدادها با داشبوردها، گزارش‌ها و اطلاع‌رسانی‌های ایمیلی

پیکربندی و توزیع آسان

- توزیع و پیکربندی یک SVM بر روی چندین Hypervisor (در معماری Agentless)
- برگرداندن فایل‌های قرنطینه‌شده با استفاده از کنسول Trellix ePO (در معماری Multiplatform)
- جزییات جامع برای میزان‌سازی کارایی ضدویروس

	معماری Multiplatform	معماری Agentless
بسترهای مجازی‌سازی پشتیبانی‌شده	تمامی بسترهای مجازی‌سازی رایج شامل VMware، Citrix، Hyper-V و KVM	VMware
بستر پویشگر	Windows Server 2012 R2، Windows Server 2016، Windows Server 2019، Windows Server 2022، Windows 8.1، Windows 10، Windows 11	Linux Ubuntu 18.04
مقایس‌پذیری و افزونگی	یک SVM قادر به حفاظت از ماشین‌های مجازی بر روی چندین Hypervisor است. بسته به ساختار، تعداد ماشین‌های SVM قابل تغییر است.	یک SVM به ازای هر ماشین میزبان ESXi
نحوه ارتباط با ماشین‌های مجازی	ارتباط از طریق شبکه	ارتباط از طریق Hypervisor
سیستم‌های عامل پشتیبانی‌شده (بر روی ماشین مجازی)	Windows	Linux و Windows

شرکت مهندسی شبکه گستر
تهران بلوار نلسون ماندلا خیابان دستگردی (ظفر) شماره ۲۷۳
www.shabakeh.net info@shabakeh.net ۰۲۱ – ۴۲۰۵۲
شبکه گستر
امنیت شما | وظیفه ما