آنتی ویروس مناسب برای مجازی سازی

مجموعه شرکت های دانش بنیان رها

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۴ www.rahaco.net

فهرست

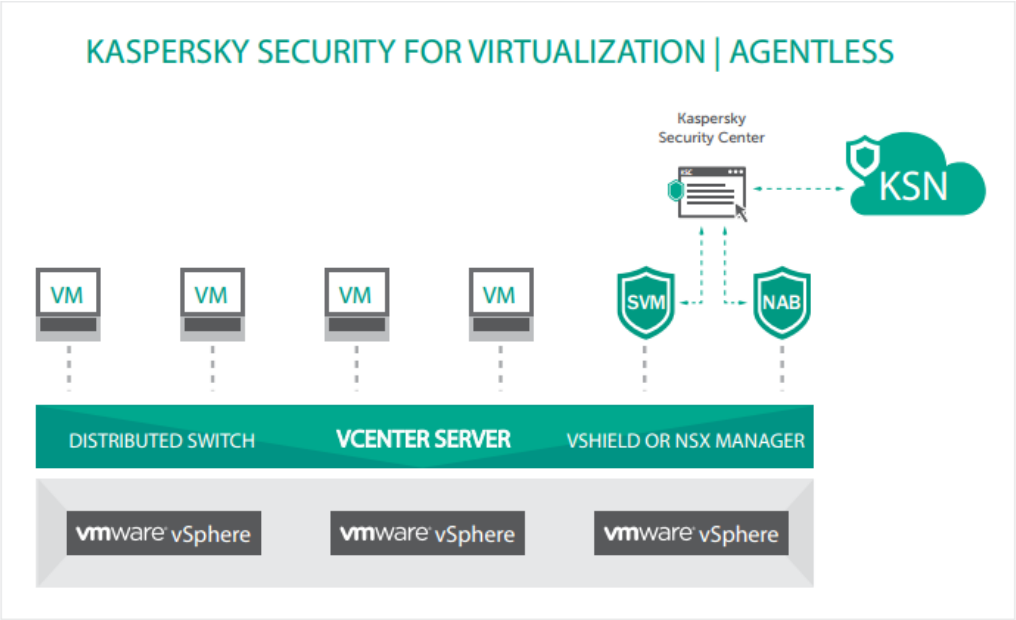
آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۴ www.rahaco.net

آنتی ویروس مناسب برای مجازی سازی

تکنولوژی مجازی سازی در ابتدا برای کاربردهای مهم و مقاصد تجاری استفاده نمی شد. تا مدتها از مجازی سازی برای کارهای موقتی و مراکز آموزشی استفاده می شد، در چنین شرایطی نیاز چندانی به امنیت احساس نمی شد چون در صورت بروز هرگونه مشکلی، ماشین های مجازی به آسانی بازسازی می شدند. با گذشت زمان و پیشرفت تکنولوژی مجازی سازی و افزایش امکانات و قابلیت های آن از یک طرف و محدودیت خرید و نصب سرورهای فیزیکی از طرف دیگر، روند جایگزینی سرورها و شبکه های فیزیکی با محیط مجازی روز به روز افزایش می یافت و همزمان با آن، مسئله امنیت محیط های مجازی و اینکه کدام آنتی ویروس مناسب برای مجازی سازی است از اهمیت بیشتری برخوردار می گشت.

شرکت های مختلفی از جمله **Kaspersky**، **McAfee** و **Trend Micro** آنتی ویروس های لایه Hypervisor تولید می کنند.

در این مقاله به صورت تخصصی‌تر به معرفی محصولات Kaspersky در حوزه امنیت Hypervisor می‌پردازیم.



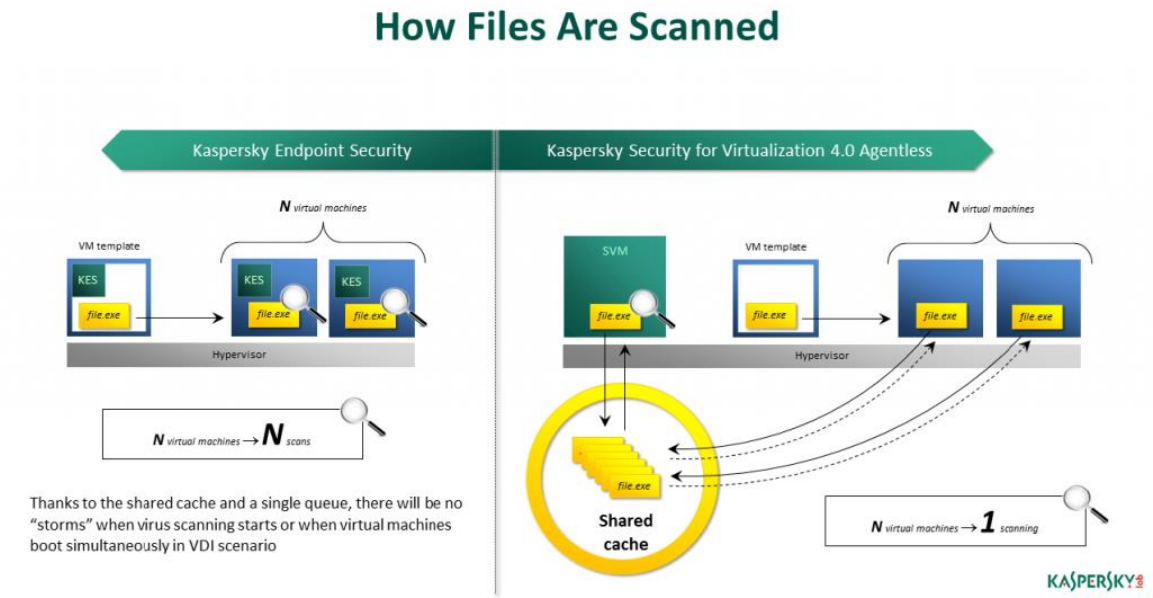
آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۴ www.rahaco.net

راهکارهای محافظت از سرورهای مجازی:

KASPERSKY SECURTY FOR VIRTUALIZATION | AGENTLESS

این محصول به طور خاص برای مجازی ساز VMware vSphere طراحی شده و در ترکیب با دو محصول امنیتی خود VMware به نام VShield و NSX کار می‌کند. این محصول امنیتی نه در داخل ماشین های مجازی بلکه در خارج از ماشین ها و داخل سرور نصب می‌شود و منابع ماشین مجازی درگیر پروسه امنیت و اسکن نخواهد شد.

این محصول مستقل از سیستم عامل ها به محافظت از سرور پرداخته و ترافیک عبوری به سیستم عامل ها را مانیتور کرده و امنیت آن ها را در برابر بد افزار ها تامین می‌کند. از مزیت های این محصول این است که فایل های مشترک بین ماشین ها را فقط یک بار اسکن می‌کند که باعث مصرف کمتر منابع سرور خواهد شد در حالی که اگر از محصولات ENDPOINT یا سایر آنتی ویروس های تحت شبکه استفاده کنیم فایل های مشترک در هر ماشین به صورت جداگانه اسکن و باعث بار اضافه روی سرور می‌شود.



آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۴ www.rahaco.net

برای حفاظت از شبکه های پیشرفته ممکن است یک SVM (Security Virtual Machine) دوم نیز در ترکیب با NSXبه منظور مسدود کردن Network Attack ها استفاده شود.

با وجود مزایای بسیار، این محصول محدودیت های نیز به همراه دارد از جمله:

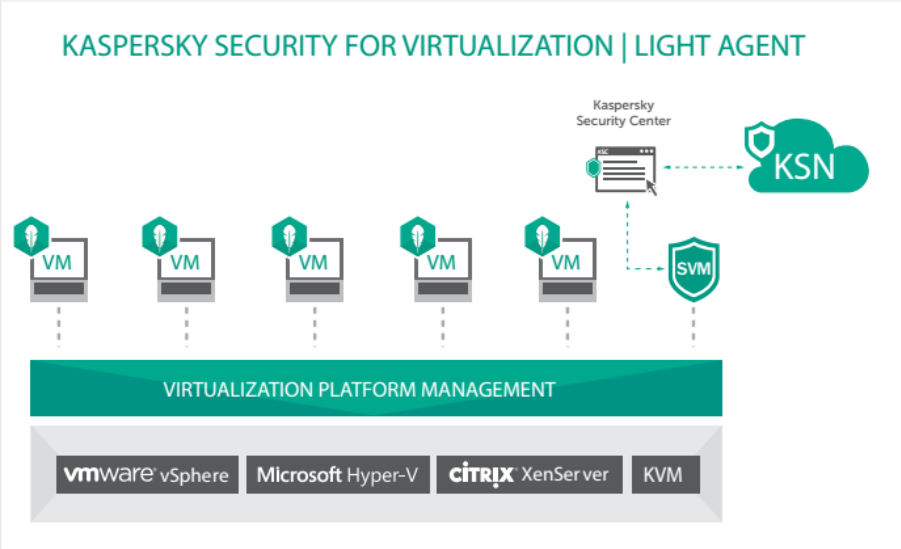
VMware vSphere –تنها پلت فرم مجازی سازی است که این محصول را ساپورت می کند، برای سایر مجازی سازها مانند Hyper-v یا Citrix XenServer باید روی ماشین هاAgent ای نصب شود.

–به دلیل معماری و ساختارVMware ، محصولات vShield و NSX دسترسی به پردازش های درون ماشین ها، اپلیکیشن ها و ترافیک های وب را فراهم نمی کنند که باعث کاهش توانایی Deep Protection (محافظت عمیق) خواهد شد.

KASPERSKY SECURTY FOR VIRTUALIZATION | LIGHT AGENT

رویکرد "Light Agent" این محدودیت هارا برطرف می کند. رویکردی مابین روش سنتی (Endpoin) و AgentLessکه مصرف منابع آن به طور چشمگیری کمتر از محصولات Endpoint و البته نه چندان بیشتر از AgentLessاست. این Agent سبک در هر VM به حافظه، اپلیکیشن ها، پردازش های داخلی، ترافیک وب و دیوایس های مجازی دسترسی دارد واجازه پیاده سازی تکنیک های پیشرفته امنیتی را در سطح ماشین به ما می دهد. همچنین این محصول از محبوب ترین پلت فرم های مجازی سازی یعنی:

Citrix XenServer، Microsoft Hyper-v، VMwareو KVM پشتیبانی می کند.



آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۴ www.rahaco.net

این محصول در محیط های مجازی از تکنولوژی های پیشرفته ای مانند HIPS (HostBased Intrusion Prevention System)و همچنین firewall بهره میبرد که شبکه ما را در برابر حملات حفاظت میکند.

این محصول برای محیط های مجازی و VDI قابلیت های جامع حفاظت از شبکه و مجموعه ای کامل از کنترل هارا بدون تاثیر محسوسی بر Hypervisor ارایه میدهد که نه تنها سیستم شما را در برابر ویروس ها ایمن میکند بلکه استفاده از نرم افزار ها، دستگاه ها یا وب سایت های نامعتبر را محدود میکند.

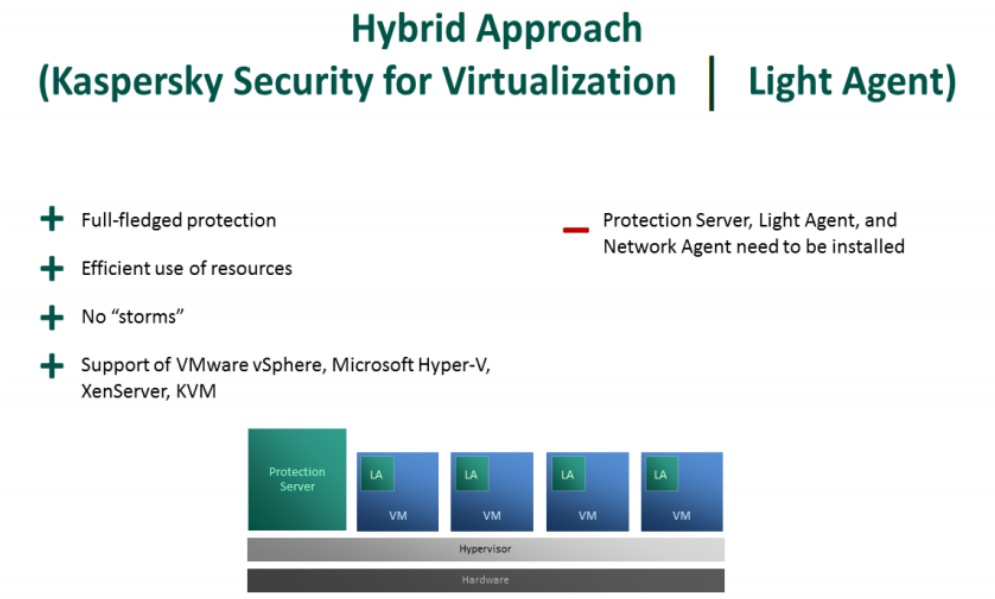
این محیط دفاعی چند لایه قدرتمند که توانایی حذف نرم افزارهای مخرب پیچیده و حتی تهدیدات صفر روز (zero-day threats)را دارد توسط تکنولوژی AEP (Automatic Exploit Prevention) تولید شده است.

مزایای light agent

-با دسترسی کامل به منابع ماشین از طریق یک Agent سبک، بالاترین سطح امنیتی و حفاظتی را دارد.

-از هر سه پلتفرم مجازی سازیVMware ، Hyper-vو Citrix پشتیبانی میکند.

-وجود لایه های امنیتی اضافی مانند HIPS و.White list



آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۴ www.rahaco.net

??? Agentless or Light agent: which is better

پاسخ به این سوال کمی پیچیده است.

با این که رویکرد Light Agent با ساختار چند لایه ای که دارد از نظر امنیتی قوی تر به نظر میرسد اما نمی تواند امنیت آنی یعنی محافظت از ماشین ها دقیقا از لحظه استارت شدن را فراهم کند، این موضوع مهمی است چرا که اگر ماشین از قبل آلوده باشد ممکن است این آلودگی را گسترش دهد و خطرات احتمالی را برای کل شبکه به وجود آورد، اما رویکرد Agentless با تامین امنیت آنی می تواند از این نظر به ما اطمینان خاطر دهد.

به این نکته هم توجه داشته باشید که برای استفاده از رویکرد Agentless باید هزینه ای اضافی برای لایسنس vShieldنیز پرداخت کنید.

موضوع دیگر محدود بودن راهکار Agentless به VMware است که بر روی مجازی سازهای Citrix و Hyper-v قابل پیاده سازی نیست. از طرفی زمانی که VDI در شبکه مان است رویکرد Light Agent بهتر خواهد بود.

با این وجود شما میتوانید ترکیبی از هردو راهکار را استفاده کنید، صرف نظر از از این که از مجازی ساز چه کمپانی ای استفاده میکنید تمامی این محصولات می توانند توسط یک واحد مدیریت مرکزی تحت عنوان KASPERSKY SECURITY CENTERمدیریت شوند.

منابع:

1. ***Kaspersky Lab. (2016). Kaspersky-virtualization-security-features-guide.pdf***
2. ***https://support.kaspersky.com/learning/courses/kl_131.30***
3. ***۳ .شرکت ایدکو، Virtualization-Security:Understanding-the-difference.pdf***

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۴ www.rahaco.net