KASPERSKY lab

WERELDWIJDE BEVEILIGINGS-INTELLIGENTIE

SECURITY FOR VIRTUALIZATION: DE JUISTE BALANS ZOEKEN

Beveiliging én prestaties in uw virtualisatieomgeving

#EnterpriseSec
kaspersky.com/enterprise

INHOUD

INLEIDING

VIRTUALISATIE HEEFT DE IT-OMGEVING VAN BEDRIJVEN GEHEEL VERANDERD

Organisaties hebben wereldwijd meer dan ooit te maken met cyberdreigingen. Het is van essentieel belang dat de IT-infrastructuur zowel fysiek als virtueel volledig en effectief beveiligd is.

Door beveiligingsfunctionaliteit aan een IT-systeem toe te voegen wordt er in een bepaalde mate gebruikgemaakt van systeembronnen. Het streven is altijd de beveiliging zo optimaal mogelijk te maken terwijl tegelijk de impact op prestaties zoveel mogelijk wordt beperkt. Het is dus nodig de juiste balans tussen beveiliging en efficiëntie van de systemen te zoeken.

Dit is met name van groot belang voor virtuele infrastructuren. De grootste voordelen van virtualisatie voor bedrijven zijn de prestatie-efficiëntie en optimalisatiewinsten, en de bijbehorende kostenbesparingen. Wanneer er op systemen beveiligingsoplossingen worden geïnstalleerd die veel van de systeembronnen vergen, kunnen deze voordelen veel kleiner worden, zodat de investering in virtualisatie zijn doel voorbijschiet.

Het is niet eenvoudig de juiste beveiligingsoplossing voor een specifieke virtuele omgeving te kiezen. Gebruik dit artikel bij het zoeken van de juiste beveiligingsstrategie voor uw virtuele omgeving: een strategie waarbij beveiliging en prestaties met elkaar in balans zijn. Omdat de “juiste balans” voor elke organisatie zal verschillen, bestaat er niet één oplossing. Maar wat in de eerste plaats belangrijk is voor een goede balans, is de aanwezigheid van – en het type – beveiligingsagent bij het virtuele endpoint; de balans tussen de mogelijkheid beveiligingsfuncties in te schakelen bij het endpoint en de hoeveelheid waardevolle verwerkingsruimte die hiervoor nodig is.

Dit artikel bevat informatie over drie beveiligingsmethoden voor de beveiliging van virtuele endpoints en het effect van de methoden op het behalen van het beste investeringsrendement. Verder worden er enkele adviezen gegeven om de beste balans tussen prestaties en beveiliging voor uw virtuele systemen en uw fysieke en mobiele omgevingen te vinden.

De drie methoden zijn:
- Agent-based
- Agentless
- Light agent

Om de juiste balans voor uw situatie te vinden is het belangrijk deze methoden te begrijpen en de sterke en zwakke punten ervan te kennen.

VIRTUALISATIE

VOLGENS EEN RECENT ONDERZOEK VAN GARTNER WAS BIJ IETS MEER DAN 60% VAN DE ONDERVRAAGDEN SPRAKE VAN TEN MINSTE ÉÉN VORM VAN DESKTOPVIRTUALISATIE.[1]

GARTNER VOORSPELT VOOR 2014 EEN TOTALE GROEI VAN 13,14% OP DE INTERNATIONALE BEDRIJFSMARKT VOOR GEHOSTE VIRTUELE DESKTOPS. VOLGENS GARTNER ZAL DE GROEI NOG TOENEMEN TOT 7,38% IN 2017.[2]

Het virtualiseren van servers en desktops kan bedrijven enorme voordelen opleveren.

Een aantal goede voorbeelden:

- Kostenbeheersing: virtualisatie verkleint de voetafdruk van hardware, de uitgaven aan hardware, de benodigde ruimte, energieverbruik, beheervereisten, enzovoort.
- Snelheid: virtualisatie vergroot de snelheid van IT dankzij nieuwe capaciteit on demand. Deze flexibiliteit kan uiteindelijk leiden tot een betere concurrentiepositie van het hele bedrijf.
- Stabiliteit: eenvoudigere, gestandaardiseerde, redundante systemen zorgen voor meer veerkracht en betere systeembeschikbaarheid, zodat medewerkers productiever zijn, waar en wanneer ze ook werken.
- Gecentraliseerd beheer: virtuele systemen kunnen direct worden gecreëerd en centraal worden beheerd en geconfigureerd, waardoor de kosten voor beheer en ondersteuning worden gereduceerd.

Samengevat gebruiken bedrijven virtualisatie omdat hiermee de efficiëntie van IT wordt geoptimaliseerd, waardoor de kosten worden verlaagd.

1 Market Trends: Desktop Virtualization, 2013, 10 oktober 2013 – Gartner, Inc.
2 Forecast: Enterprise Software Markets, Worldwide, 2010 – 2017, Q413 Update – Gartner, Inc.

VIRTUELE BEVEILIGING: DE RISICO'S

BEGIN 2011 BEVATTE DE MASTERDATABASE VAN KASPERSKY 35 MILJOEN DREIGINGEN. EEN JAAR LATER IS DE INHOUD VAN DEZE DATABASE BIJNA VERDUBBELD NAAR 67 MILJOEN. GEMIDDELD ONTDEKT KASPERSKY NU PER DAG 315.000 NIEUWE DREIGINGEN.

ZIJN VIRTUELE MACHINES (VM's) VAN ZICHZELF VEILIGER DAN FYSIEKE SYSTEMEN?

Het antwoord is nee. Er zijn misschien enkele infectiehaarden waartegen VM's beter bestand zijn (bijvoorbeeld ransomeware-dreigingen voor virtuele servers), maar verder zijn VM's net zo kwetsbaar voor de meeste vormen van malware, waaronder schadelijke e-mailbijlagen, drive-by-downloads, botnet trojans, netwerkwormen en zelfs gerichte “spear-fishing”-aanvallen.

Deze dreigingen blijven bestaan zolang het virtuele systeem actief en in gebruik is.

Het National Institute of Standards and Technology zegt:

"Virtualisatie zorgt voor extra lagen technologie en daardoor kan de last van beveiligingsbeheer toenemen omdat hiervoor aanvullende middelen nodig zijn. Als meerdere systemen in één fysieke computer worden gecombineerd, is het potentiële effect groter als de beveiliging wordt doorbroken. Verder vormen virtualisatiesystemen, die werken met een gedeelde resource-infrastructuur, een gevaarlijke infectiehaard doordat één geïnfecteerde VM de volledige virtuele infrastructuur kan besmetten."[3]

Er zijn nog meer risico's voor de virtuele omgeving:

- Netwerkbesmetting: malware, die onschadelijk is gemaakt op een niet-persistente VM toen deze werd uitgeschakeld, heeft via het virtuele netwerk waarschijnlijk al andere machines geïnfecteerd. Gezien de snelheden die in deze netwerken mogelijk zijn, kan de infectie razendsnel uitbreiden en nieuwe machines tijdens het opstarten besmetten.
- Opslagbesmetting: malware kan zich ook verspreiden door de opslagruimtes te infecteren waartoe VM's toegang krijgen.
- Een VM kan worden gebruikt om het verkeer van een andere VM "af te luisteren".
- Malwareontwikkelaars kunnen hun aanvalsstrategie ook uitbreiden door code te schrijven die op zowel fysieke als virtuele systemen gericht is.

MALWAREDREIGINGEN VOLGEN ELKAAR IN EEN ALARMEREND HOOG TEMPO OP

Begin 2011 bevatte de masterdatabase van Kaspersky 35 miljoen dreigingen. Een jaar later is de inhoud van deze database bijna verdubbeld naar 67 miljoen. Gemiddeld ontdekt Kaspersky Lab nu per dag 315.000 nieuwe dreigingen.

De op organisaties gerichte wapens van cyber-warfare, van hit-and-run aanvallen op de toeleveringsketen tot “watering-hole attacks”, waarbij spear phishing en drive-by downloads worden gecombineerd, worden steeds geavanceerder. Geen enkel bedrijf is immuun.

"Elke organisatie kan het slachtoffer worden. Alle organisaties hebben gegevens die waardevol kunnen zijn voor cybercriminelen en die ook als “opstap” kunnen worden gebruikt om andere bedrijven te bereiken."
David Emm van het Kaspersky GReAT (Global Research and Analysis) Team[4]

Kortom, er is zowel in de fysieke als virtuele wereld nog nooit zo'n grote behoefte geweest aan hoogwaardige beveiliging als nu.

Omdat de virtualisatietechnologie nu in veel bedrijven wordt gebruikt, en met name in grote ondernemingen die over veel waardevolle informatie beschikken, hebben cybercriminelen alle reden om hun spel te verbeteren en nog meer moeite te doen om virtuele systemen te infiltreren, besmetten en manipuleren.

3 Guide to Security for Full Virtualization Technologies, National Institute of Standards & Technology, 2011
4 Kaspersky Security Bulletin 2013

VIRTUELE BEVEILIGING: DE BALANS

Organisaties investeren in virtualisatie om de efficiëntie te verhogen en kosten te verlagen. De geoptimaliseerde prestaties die tot kostenbesparingen leiden, moeten behouden blijven. En één element dat tot op zekere hoogte de capaciteit van systemen verbruikt, is de beveiligingssoftware.

Het is gewoon een feit dat sommige anti-virusimplementaties de virtuele infrastructuur verstoppen, waardoor consolidatieratio's afnemen en het investeringsrendement of de ROI in gevaar komt. Eén whitepaper over beveiligingsbenchmarking stelt dat bepaalde anti-virusconfiguraties de capaciteit op de virtuele desktophost met 40% kunnen verminderen.[5]

Maar het is ook een feit dat virtuele systemen kwetsbaar zijn voor cyberdreigingen en moeten worden beschermd. Wat de kosten ook zijn om beveiliging te implementeren, de kosten van een grote inbreuk op de beveiliging van een bedrijf zullen waarschijnlijk nog veel hoger zijn. Een dergelijke inbreuk kan een bedreiging voor de hele organisatie vormen. Denk alleen al aan de gevolgen voor de reputatie van het bedrijf.

De mythe dat virtuele omgevingen van zichzelf veilig zijn en niet hoeven worden beschermd, is nu grotendeels onjuist gebleken. Dit is deels te wijten aan de inspanningen van cybercriminelen wereldwijd, die al langer de vele kansen die gevirtualiseerde systemen bieden in het oog hielden en deze kansen nu benutten (Morcut, of Crisis, de eerste trojan die op VM's gericht was, werd al in 2012 geïdentificeerd).

Toch is er terughoudendheid om - in dezelfde mate als voor fysieke systemen - te investeren in beveiliging voor gevirtualiseerde systemen.

Wat zijn de redenen van de ogenschijnlijke paradox “snel met virtualisatie, traag met beveiliging”? Gartner verwoordt de kern van dit probleem:

"De beveiliging van een [virtueel] platform brengt kosten met zich mee, niet alleen wat betreft licenties voor beveiligingssoftware, maar ook in de vorm van mogelijk negatieve impact op de prestaties. Producten waarmee op malware wordt gescand, kunnen de capaciteit van het platform aanzienlijk verminderen, met name als de producten niet optimaal voor de omgeving zijn geconfigureerd." [6]

De primaire redenen om in virtualisatie te investeren, zijn de toegenomen prestatie-efficiëntie en haalbare kostenbesparingen. Als de capaciteit van het platform verslechtert door verkeerd ontworpen en geconfigureerde beveiligingssoftware, is die reden niet meer geldig.

Tot nu toe vormen alle opties die beschikbaar zijn om VM's tegen malware te beschermen een ongelukkig compromis tussen beveiliging, prestaties en beheer.

Maar wat kan de verstandige IT-beheerder nu precies doen om een efficiënte maar goed beschermde virtuele omgeving in stand te houden en toch de volledige bedrijfsvoordelen van virtualisatie te realiseren? Wat is een goede balans en hoe realiseert u dit?

Het antwoord is dat het beveiligingssysteem goed moet zijn ontworpen: de architectuur van het systeem moet geschikt zijn voor de specifieke beperkingen van virtuele omgevingen, met name wat betreft de aanwezigheid en functionaliteit van een beveiligingsagent bij het virtuele endpoint.

Laten we eens bekijken welke drie beveiligingsmethoden beschikbaar zijn: agent-based, agentless en light agent.

5 Phase 5 – Antivirus and best practices on VDI V1, januari 2013, Project Virtual Reality Check (VRC)
6 Know the Security Implications of Adopting Hosted Virtual Desktops, 8 april 2013 – Gartner, Inc.

DE AGENT-BASED OPTIE

Een mogelijke aanpak is het gebruik van een traditionele, agent-based beveiligingsoplossing. Hierbij wordt een volledige kopie van de anti-virussoftware op elke VM geladen, net als bij de meeste beveiligingsoplossingen voor fysieke endpoints.

Deze aanpak kan een redelijk hoog beveiligingsniveau leveren, maar er wordt meestal veel van de systeembronnen en de prestaties gevergd wanneer software die is ontworpen voor fysieke omgevingen, door gedeelde bronnen wordt gebruikt.

DE VOORDELEN

- Wanneer een ouder fysiek beveiligingssysteem voor de virtuele omgeving wordt gebruikt, heeft het als voordeel dat dit vertrouwd is en dat er geen nieuw inkoopproces hoeft te worden gestart.
- Schaalvoordelen en efficiëntiebesparingen kunnen worden gerealiseerd door één beveiligingssysteem voor zowel fysieke als virtuele omgevingen te gebruiken.
- Organisaties met slechts enkele VM's en geen plannen om meer in gebruik te nemen, zien mogelijk geen reden te investeren in beveiligingssoftware die specifiek voor virtualisatie bestemd is.

DE BEPERKINGEN

Verslechtering van de prestaties

Als de anti-virussoftware en definitiedatabase op elke VM worden geladen, kunnen de prestaties van de virtuele systemen aanzienlijk verslechteren. Duplicatie van definitiedatabases en redundante bestandsscans maken onnodig gebruik van waardevolle systeembronnen, en deze en andere onderliggende redundanties hebben een negatieve invloed op de beschikbaarheid van geheugen, opslagruimte en CPU, en verhogen het brongebruik waardoor consolidatieratio's afnemen.

Bronconflicten en “AV-stormen”

Als elke agent voor een virtueel endpoint onafhankelijk alle beveiligingstaken uitvoert, ontstaan er bronconflicten.

Symptomen zijn onder andere:

- **Scanstormen** – op het moment dat meerdere VM's tegelijkertijd met een geplande scan beginnen, is het mogelijk dat de verwerkingskracht van het hostsysteem hierop niet berekend is en er problemen met hostgebruik en prestaties optreden (de host kan zelfs crashen).
- **Updatestormen** – net als bij scanstormen kunnen zich updatestormen voordoen wanneer alle VM's met een lokale definitiedatabase tegelijkertijd updates proberen te downloaden en te installeren.

Beveiligingsproblemen

VM's kunnen eenvoudig offline worden gehaald en lange perioden inactief zijn. Wanneer de VM's weer online worden gehaald (geactiveerd), kan er sprake zijn van beveiligingsproblemen, zoals niet-gepatchte softwarevulnerability's en verouderde definitiedatabases, waardoor de systemen kwetsbaar zijn en een mogelijk doelwit van cybercriminelen worden.

Incompatibiliteit

Virtuele en fysieke systemen verschillen op belangrijke punten: bijvoorbeeld het gebruik van niet-persistente schijven en het live VM-migratieproces. Standaard anti-malwareproducten die zijn ontworpen voor fysieke endpoints, houden vaak geen rekening met eigenschappen van virtuele omgevingen en machines, en kunnen daarom leiden tot onverwachte vertragingen en fouten. Ook is het mogelijk dat dergelijke producten helemaal niet kunnen worden uitgevoerd.

Incompatibiliteit is niet onvermijdelijk. De oplossing Endpoint Security for Business van Kaspersky is ontworpen met de achterliggende gedachte dat er organisaties zijn die dezelfde agent-based oplossing voor zowel fysieke als virtuele infrastructuren willen gebruiken. Kaspersky Endpoint Security for Business kan daarom probleemloos en effectief in gevirtualiseerde omgevingen worden gebruikt en door specifieke aanpassingen die zijn ontworpen om de prestaties van virtuele systemen te optimaliseren, is Kaspersky Endpoint Security for Business bij uitstek geschikt wanneer de voorkeur uitgaat naar een agent-based oplossing.

DE BALANS

Een agent-based optie is niet optimaal voor de prestatie-efficiëntie omdat de VM-dichtheid wordt gereduceerd en het investeringsrendement nadelig wordt beïnvloed. Bij de agent-based optie worden de systemen waarschijnlijk goed genoeg beveiligd, maar dit gaat ten koste van systeembronnen, wat de meeste organisaties die virtualisatietechnologie implementeren onwenselijk vinden.

DE AGENTLESS OPTIE

De agents van traditionele beveiligingssoftware vragen gewoon teveel van de systeembronnen en zijn niet flexibel in VM-omgevingen. Stel dat er beveiliging voor virtuele systemen zou kunnen worden geïmplementeerd zonder dat er een endpoint-agent nodig is?

Dit is mogelijk als het beveiligingssysteem nauw geïntegreerd is met het virtualisatieplatform en de functionaliteit van het platform kan gebruiken om met afzonderlijke VM's te communiceren.

Er kan dan één aparte virtuele applicatie worden gebruikt om anti-malwarebeveiliging voor alle VM's te bieden.

DE VOORDELEN

- Door alle scanverwerking van de afzonderlijke VM's te halen, wordt de algehele geheugenfootprint heel klein, zodat de mogelijkheden van de fysieke hardware worden uitgebreid en de consolidatiedichtheid toeneemt.
- De aanmaak van een nieuwe machine leidt niet tot vulnerability aangezien de virtuele beveiligingsapplicatie zichzelf continu bijwerkt.
- Aangezien alleen de virtuele beveiligingsapplicatie viruscontroles uitvoert en updates van de beveiligingsleverancier ontvangt, worden AV-stormen gemakkelijk vermeden en is het I/O-verbruik beperkt.

DE BEPERKINGEN

Deze agentless benadering levert weliswaar een beter investeringsrendement op, maar kent ook een aantal beperkingen.

Ondersteunde platformen

De agentless benadering is momenteel alleen mogelijk in VMware-omgevingen, waar de vShield-endpointfaciliteit is ontwikkeld met dit in gedachten. vShield kent echter eigen beperkingen voor de beveiligingsniveaus die kunnen worden geïmplementeerd. Wat belangrijk is om te weten, is dat vShield de beveiligingsoplossing met VM-toegang alleen op het niveau van bestandssystemen levert.

Minder uitgebreide bescherming

Zonder volledige toegang tot afzonderlijke VM-activiteiten en -gegevens via een bepaalde vorm van een agent kunnen de endpointbeveiliging en het beheer niet worden geïmplementeerd.

Moderne agent-based anti-malwaresoftware zou gelaagde beveiligingsmodules moeten bevatten, zoals applicatiebeheer, webfilters, een Host-based Intrusion Prevention System (HIPS), persoonlijke firewall en meer, die allemaal een bepaalde vorm van een endpoint-agent nodig hebben.

Natuurlijk is een beveiligingssysteem zo goed als de dreigingsintelligentie die het systeem informatie verschaft en de anti-malware-engine die het systeem beschermt. Daarom is een optimale basis voor anti-malwarebeveiliging van cruciaal belang voor elk beveiligingssysteem – agent-based of niet.

Maar als een meerlaagse benadering door de implementatie van deze robuuste tools niet kan, moet de resterende engine voor anti-malwaredetectie zo krachtig en intelligent mogelijk zijn.

Geen enkele anti-malware-engine kan echter concurreren met de beschikbare beveiligingsniveaus wanneer toegang kan worden verkregen tot VM-geheugens en -processen. Agentless oplossingen die speciaal zijn ontwikkeld voor virtuele omgevingen, zijn minder uitgebreid en bieden alleen de traditionele bescherming tegen malware.

Apart beheer van beveiligingssystemen

Tegenwoordig onderhouden de meeste organisaties die virtualisatie gebruiken zowel fysieke als virtuele omgevingen.

Als er twee aparte beveiligingssystemen worden gebruikt (één voor virtuele en één voor fysieke systemen), zijn er ook twee aparte beheerconsoles nodig. Het beleid moet dan apart in de twee omgevingen worden geïmplementeerd en rapportages moeten handmatig worden samengevoegd om een algeheel beeld van de beveiliging te krijgen.

Door twee parallelle maar afzonderlijk beheerde systemen te implementeren, nemen de kosten waarschijnlijk toe door een verdubbeling van de beheerkosten en wordt de kans op fouten groter.

Dit hoeft echter niet altijd het geval te zijn. Bij de Kaspersky-methode, waar sprake is van één geïntegreerd platform, zijn de virtuele en fysieke beveiligingsoplossingen naadloos geïntegreerd en worden ze samen via één console beheerd.

DE BALANS

Er zijn situaties waarin een agentless oplossing de efficiëntste optie is. Eén voorbeeld is een situatie waarin virtuele servers voor opslag- en databasebeheeractiviteiten worden gebruikt. Voor deze zwaarbelaste interne omgevingen, waarin machinedichtheid een belangrijke factor is en de systemen zeer beperkt aan dreigingen worden blootgesteld, heeft het optimaliseren van prestaties door het gebruik van een agentless oplossing hogere prioriteit.

Maar de risico's moeten goed worden afgewogen. Als er alleen op de anti-malware-engine wordt vertrouwd, zijn natuurlijk de uitgebreidheid en geavanceerdheid van die engine en de kwaliteit van de dreigingsintelligentie die de informatie verschaft, van het allergrootste belang.

DE LIGHT AGENT OPTIE

Bij de lichte vorm van agent-based beveiliging voor virtuele omgevingen worden de prestatievoordelen van de agentless oplossing gecombineerd met de meerlaagse beveiligingsmethode van de beste agent-based beveiligingssystemen.

Wanneer is een agent een “light agent”? Als de mogelijkheden van de agent beperkt zijn tot alleen die functies die op het endpoint nodig zijn. Net als bij de agentless methode wordt ook een aparte virtuele beveiligingsapplicatie geïnstalleerd en met deze applicatie worden alle zware taken uitgevoerd. De “light agent” die op de VM wordt geïnstalleerd, verricht voor zover mogelijk de lichtste taken, zodat de impact van de agent op systeemprestaties tot het absolute minimum wordt beperkt.

DE VOORDELEN

Meerlaagse beveiliging

Doordat er een light agent aanwezig is, is het nu mogelijk geavanceerde endpointbeveiliging en beheerfuncties aan de oplossing toe te voegen, waaronder:

Beheer

Er is een toolbox met beheeropties voor endpoints beschikbaar.

- Afzonderlijke toegang tot specifieke applicaties kan worden geblokkeerd, gereguleerd of toegestaan, waardoor de mogelijkheden van besmetting door malware via onbekende of niet-gepatchte vulnerability's in hoge mate worden beperkt. Dit geldt met name als er sprake is van een “Default Deny”-scenario.
- Schadelijke of niet-werkgerelateerde websites kunnen worden geblokkeerd of gereguleerd, waardoor de productiviteit van gebruikers toeneemt en de beveiliging wordt verbeterd door controle op niet-toegestane en tijdverspillende online activiteiten.
- De verbinding van randapparatuur kan worden beperkt of geblokkeerd, waardoor het niet mogelijk is malware te uploaden of bedrijfsgegevens te downloaden.

Aanvullende beveiligingstechnologieën

HIPS (Host Based Intrusion Prevention System) – controle van zowel systeem- als netwerkgedrag en actieve bescherming tegen aanvallen die gericht zijn op het VM-geheugen.

Een hostgebaseerde firewall die de verspreiding van malwarebesmetting helpt voorkomen door netwerktoegang op systeemniveau te beperken.

Een light agent-oplossing kan volledig samenwerken met beveiligingstechnologieën met cloudondersteuning, waardoor geavanceerde technologieën zoals AEP (Advanced Exploit Prevention) en BSS (Behavior Stream Signatures) mogelijk zijn. De kwaliteit van de anti-malware-engine blijft van het allergrootste belang, maar bij virtuele beveiliging kan nu de volledige bescherming van beveiligingstechnologieën worden geïmplementeerd die ook bij fysieke IT-omgevingen mogelijk is.

Prestatie-efficiëntie

Door een aparte virtuele beveiligingsapplicatie te installeren kunnen de meeste prestatie-efficiënties worden gerepliceerd die met een agentless oplossing worden gerealiseerd.

- Hypervisor I/O, CPU en geheugengebruik zijn allemaal geminimaliseerd. Aangezien updates door één virtuele applicatie worden verwerkt in plaats van door elke VM, worden AV-stormen vermeden. Als de ene applicatie continu updates verwerkt, wordt bovendien de vulnerability op machineniveau tot een minimum teruggebracht en wordt er meteen up-to-date beveiliging toegepast.

  In het geval van Kaspersky Security for Virtualization is dit continue updateproces dat directe dreigingsbeveiliging biedt met behulp van het Kaspersky Security Network met cloudondersteuning, een bijzonder intensief proces. Daarom is de centralisatie van dit proces van cruciaal belang.

- Er kunnen cachetechnologieën worden geïmplementeerd – het resultaat van een bestandsscan kan aan alle VM's van de host beschikbaar worden gesteld, zodat er niet onnodig hoeft te worden gescand. Dit leidt tot een aanzienlijke reductie van zowel scantijd als het gebruik van systeembronnen.

DE BEPERKINGEN

Er is nog steeds een agent

Een light agent heeft natuurlijk altijd nog een grotere footprint dan helemaal geen agent.

Apart beheer van beveiligingssystemen

De meeste virtuele beveiligingsoplossingen vereisen een aparte console van de rest van de beveiligingsoplossing.
Dit is echter niet per se nodig. Denk bijvoorbeeld aan Kaspersky's unieke architectuur met slechts één platform.

Kaspersky's Security for Virtualization is gebouwd op de endpointbeveiliging voor het ene platform van Business, samen met onze fysieke beveiligingsoplossingen.

Hierdoor kunnen de fysieke en virtuele beveiliging, ook al zijn het aparte oplossingen die voor het optimaliseren van prestaties in verschillende omgevingen zijn ontworpen, samen worden beheerd via één console. Er kan een gezamenlijk beleid worden ontwikkeld en geïmplementeerd en er kunnen gezamenlijke rapporten worden gegenereerd. Er komen nauwelijks of helemaal geen extra beheertaken bij en u kunt de beveiligingsstatus van de gehele IT-omgeving in één keer overzien.

DE BALANS

Met light agent-oplossingen kan precies de balans worden gevonden tussen prestaties en bescherming zodat u het “beste van beide werelden” krijgt. Door de aanwezigheid van een agent kunt u geavanceerde beveiligings- en beheerfuncties bij het virtuele endpoint implementeren, terwijl een aparte beveiligingsapplicatie alle taken uitvoert die kunnen worden gecentraliseerd, zodat duplicatie wordt vermeden en de impact op prestaties tot een minimum wordt teruggebracht.

Een efficiënt ontworpen light agent-oplossing is meestal de beste optie wanneer het belangrijk is een goede balans te vinden tussen geavanceerde beveiliging en uitstekende prestaties.

CONCLUSIE

Bedrijven zien in dat virtualisatie grote voordelen oplevert en ze onderkennen de gevaren van zich steeds verder ontwikkelende dreigingen. Als echter het verkeerde beveiligingssysteem wordt geïnstalleerd, kan dit grote gevolgen hebben voor de prestaties van uw virtuele systemen en de mate waarin u werkelijk bent beveiligd.

De ideale beveiligingsoplossing biedt bescherming waar de oudere beveiligingsoplossingen tekortschieten, met een aanpak die te vergelijken is met de virtualisatie zelf – flexibel, aanpasbaar en met de mogelijkheid om een aanzienlijk continu investeringsrendement te leveren door uitstekende bescherming te bieden zonder op prestaties in te leveren.

Door het gebruik van Kaspersky Security for Virtualization kunt u die balans realiseren. Met Kaspersky Security for Virtualization kunt u elke gewenste combinatie van light agent, agentless en agent-based applicaties implementeren. Kaspersky Security for Virtualization biedt een superieure anti-malware-engine, de geoptimaliseerde prestatievoordelen van een efficiënt, precies afgesteld virtualisatiespecifiek ontwerp en één geïntegreerde beheermethode voor al uw beveiligingsbehoeften.

De erkende, internationale R&D-experts van Kaspersky hebben een flexibele oplossing ontwikkeld waarmee de benodigde prestatievoordelen worden geboden terwijl uw virtuele omgeving volledig beveiligd blijft. De oplossing wordt bovendien ondersteund door het beste ecosysteem voor dreigingsintelligentie ter wereld.

Het Kaspersky Security Network levert samen met onze wereldwijd befaamde Threat Research and Global Research and Analysis Teams (GReAT) optimale informatie over dreigingen uit alle hoeken van de wereld. Met deze intelligentie blijven we op de hoogte van beveiligingsincidenten en kunnen we deze vaak voorspellen, zodat bedrijven beter beschermd zijn en proactief aan hun IT-beveiliging kunnen werken. Wij richten ons volledig op het oplossen van de wereldwijde problemen met IT-beveiliging – van essentiële bescherming van infrastructuren, zakelijke mobiliteit en veilige virtualisatie tot fraudepreventie en beveiligingsintelligentieservices.

Kaspersky blijft continu anticiperen op IT-beveiligingsdreigingen om de risico's van dit moment en in de steeds complexer wordende toekomst te minimaliseren.

Over Kaspersky Lab

Kaspersky Lab is 's werelds grootste particuliere leverancier van beveiligingsoplossingen voor endpoints. Het bedrijf staat in de top 4 van wereldwijde leveranciers van beveiligingsoplossingen voor endpointgebruikers*. In zijn meer dan 16-jarige geschiedenis is Kaspersky Lab altijd innovatief op het gebied van IT-beveiliging gebleven en Kaspersky Lab levert effectieve digitale beveiligingsoplossingen voor grote ondernemingen, het MKB en consumenten. Kaspersky Lab, waarvan de holding is geregistreerd in het Verenigd Koninkrijk, is momenteel actief in bijna 200 landen en regio's over de hele wereld en levert wereldwijd beveiliging aan meer dan 300 miljoen gebruikers.

Ga voor meer informatie naar kaspersky.com/enterprise

* Het bedrijf staat op de vierde plaats in de IDC-rating Worldwide Endpoint Security Revenue by Vendor, 2012. De rating werd gepubliceerd in het IDC-rapport "Worldwide Endpoint Security 2013–2017 Forecast and 2012 Vendor Shares" (IDC #242618, augustus 2013). In het rapport worden softwareleveranciers gerangschikt op basis van de verkoopomzet voor endpointbeveiligingsoplossingen in 2012.