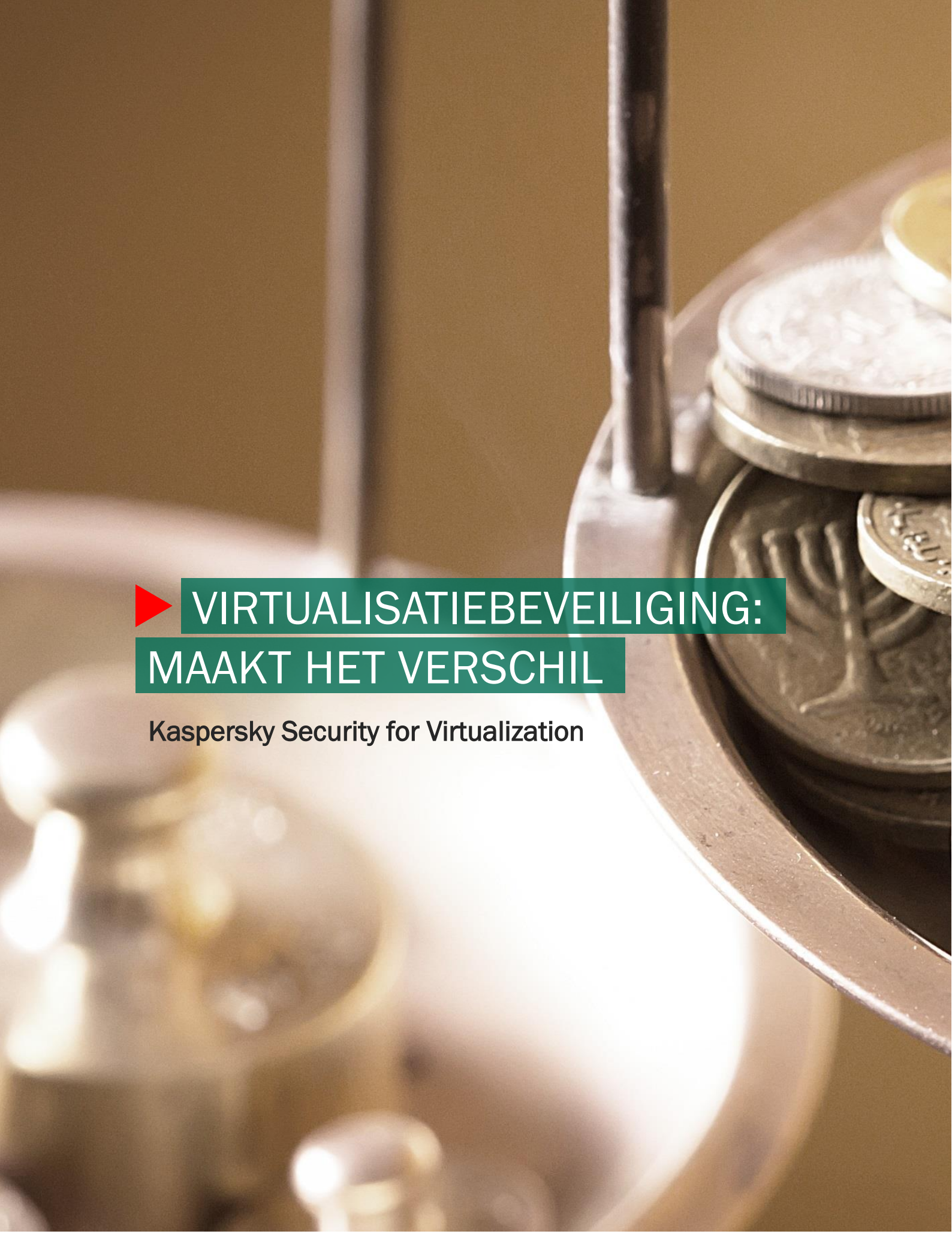


VIRTUALISATIEBEVEILIGING: MAAKT HET VERSCHIL

Kaspersky Security for Virtualization

KASPERSKY lab

Virtualisatiebeveiliging maakt het verschil

Is uw bedrijf al bezig met de transitie van fysieke naar virtuele hardware? Dan wilt u ongetwijfeld een maximale efficiëntie in uw IT-infrastructuur realiseren. Een overtuigend argument is meerdere virtuele machines (VM's) uit te voeren op één computer in plaats van gebruik te maken van aparte servers, die allemaal stroom, koeling en onderhoud nodig hebben. Het gebruik van meerdere gevirtualiseerde nodes op één fysieke server levert bedrijven een kostenbesparing op. Virtualisatie kan vanuit economisch oogpunt een krachtig effect hebben: volgens een enquête uitgevoerd door Forrester in 2011, leverde de implementatie van VDI-infrastructuur van VMware een investeringsrendement met risicocorrectie van maar liefst 255% over een periode van 4 jaar op. De investering was in 17 maanden terugverdiend.

De vraag is: hoeveel VM's kunt u in een hardwareconfiguratie kwijt zonder negatieve gevolgen voor de prestaties? Dit wordt ook wel de 'consolidatieratio' genoemd. Dit is een complex aspect van virtualisatie, aangezien diverse factoren meespelen. Wat voor taken gaan uw virtuele machines uitvoeren? Welke hypervisorsoftware gaat u implementeren? Wat zijn de risico's van het wedden op één paard? En hoe gaat u uw nieuwe virtuele infrastructuur beveiligen om uw bedrijf te beschermen tegen cybercriminelen, zonder extreme maatregelen te nemen en de boel enorm te vertragen? Om de juiste beslissing te nemen, moet u de verschillende concepten begrijpen en weten hoe deze met elkaar verband houden.

Virtualisatiemodellen

In de branche worden verschillende virtualisatiemodellen toegepast. In dit document komen de volgende drie aan bod:

- **Servervirtualisatie:** hiermee kunt u verschillende exemplaren van een besturingssysteem uitvoeren op één server. Dit is de beste manier om optimaal gebruik te maken van uw bronnen: de bezetting kan oplopen tot 80%, in vergelijking met gemiddeld 10-20% bij fysieke servers die slechts één rol vervullen[1]. **Hardwarematige servervirtualisatie** zorgt voor slechts één tussenlaag (hypervisor) tussen de virtuele machine (VM) en de hardware. Dit biedt een hogere waarde dan **softwarematige servervirtualisatie**, waarbij het onderliggende besturingssysteem extra bronnen verbruikt. Voor de meeste zakelijke applicaties verdient hardwarematige virtualisatie derhalve de voorkeur.
- **Desktopvirtualisatie** biedt een ander waardescenario door een reeks fysieke desktopsystemen te vervangen door een desktopvirtualisatie-infrastructuur oftewel Virtual Desktop Infrastructure (**VDI**). Kostenbesparende 'thin clients', rolgebaseerde externe bureaubladen, externe vestigingen zonder noodzaak van een eigen IT-service en het volledige onderhoud voor honderden werkplekken is beperkt tot slechts enkele fysieke servers.
- **Applicatievirtualisatie:** in tegenstelling tot een infrastructuur met rolgebaseerd extern bureaublad, wordt de virtuele omgeving enkel toegepast voor één applicatie. Voor de steeds populairdere Software-as-a-Service-benadering is dit een voor de hand liggende en efficiënte keuze.

Alle virtualisatiemodellen bieden talloze gebruiksmogelijkheden, elk met hun eigen risico's. Daarbij is het risico van cyberdreigingen een van de belangrijkste, waardoor het absoluut noodzakelijk is om enige vorm van beveiliging te implementeren. Deze taak wordt nog lastiger wanneer u zich realiseert dat de genoemde drie benaderingen kunnen worden toegepast binnen één IT-netwerk. Daarbij zult u echter ook rekening moeten houden met een hoger bronnenverbruik.

---

[1] - *Ruest D. Virtualization. A Beginners Guide. McGraw-Hill, 2010, pagina 4*

Er bestaan echter manieren om de impact op uw nieuwe en zeer efficiënte virtuele infrastructuur te beperken.

Een gespecialiseerde beveiligingsoplossing voor virtuele omgevingen is van essentieel belang

Uiteraard kunt u de vertrouwde agents voor endpointbescherming installeren op uw virtuele systemen. Die hebben echter een aantal belangrijke tekortkomingen die uw ervaring met gevirtualiseerde IT-infrastructuren negatief kunnen beïnvloeden.

1. **Duplicatie** Elke VM bevat een identieke set beveiligingscomponenten, zoals een geïsoleerde anti-malware-engine en definitiedatabases die elk afzonderlijk moeten worden bijgewerkt. Hierdoor wordt een aanzienlijk deel van uw kostbare bronnen (processorkracht, RAM-geheugen en schijf-storage) in zekere zin nodeloos verbruikt, waardoor de uiteindelijke consolidatieratio behoorlijk omlaag gaat.
2. **'Stormen'** Deze term wordt gebruikt voor het gelijktijdig uitvoeren van anti-malwarescans of database-updates door verschillende machines, wat kan leiden tot een plotselinge piek in bronnenverbruik. Hierdoor kunnen de prestaties afnemen of services volledig uitvallen. Met een handmatige configuratie kunt u dit probleem gedeeltelijk oplossen, maar bij grote aantallen (bijv. honderden) VM's kan handmatig ingrijpen zeer tijdrovend zijn.
3. **'Hiaat bij inschakeling'** Sommige virtuele systemen blijven inactief tot deze worden ingeschakeld. Helaas is het op een inactieve VM niet mogelijk om componenten of databases van de beveiligingsoplossing bij te werken. Dat betekent dat de VM tussen het opstarten en het doorvoeren van de beveiligingsupdate kwetsbaar is voor aanvallen.
4. **'Paniekaanvallen'** Het is gebruikelijk dat systeembeheerders als vooraf gedefinieerde reactie op een virusuitbraak de beveiliging opschroeven door over te schakelen op een 'paranoïde' modus en een ongeplande scan uit te voeren. Hoewel dergelijk beleid voor fysieke nodes zeker zinvol kan zijn, kan dit in een virtuele omgeving tot enorme systeemvertragingen leiden.
5. **Incompatibiliteitsproblemen** Virtuele machines zijn in veel opzichten vergelijkbaar met hun fysieke tegenhangers. Toch zijn er een aantal belangrijke verschillen die u in het achterhoofd moet houden, zoals het gebruik van niet-persistente schijven of het livemigratieproces van VM's. Standaardanti-malware is ontwikkeld voor fysieke endpoints en houdt geen rekening met de vele nuances die zo kenmerkend zijn voor virtuele omgevingen. Hierdoor kunnen er onverwachte vertragingen of storingen optreden of kan een VM helemaal uitvallen.

Gezien het bovenstaande lijkt het duidelijk dat er een gespecialiseerde oplossing nodig is. Bij het maken van een dergelijk product moeten bovenstaande overwegingen worden meegenomen bij het bieden van een zo hoog mogelijk beschermingsniveau zonder negatieve beïnvloeding van de algehele prestaties. Kaspersky Lab, technologisch marktleider in cyberbeveiligingsoplossingen, biedt bedrijven een optimale oplossing voor de drie populairste virtualisatieplatformen: VMware, Microsoft Hyper-V en Citrix.

Platformen en beschermingsmodi

Agentless-benadering

VMware, een van de oudste en nog steeds het populairste virtualisatieplatform, voorziet in een oplossing die vShield wordt genoemd. Hiermee kan de VM worden ontlast van het aanhouden van identieke databases en het verdubbelen van agents voor anti-malwarescans. Dit wordt agentless-benadering genoemd.

Kaspersky Lab biedt een gespecialiseerde beveiligingsoplossing voor VMware-platformen: **Kaspersky Security for Virtualization | Agentless.** Bij deze oplossing worden de scanfuncties uitgevoerd door één Security Virtual Appliance (SVA), een gespecialiseerde virtuele machine waarop zowel de scan-engine als de beveiligingsdatabases staan. Deze beschermt alle VM's die op de hypervisor worden uitgevoerd.

De voordelen zijn duidelijk:

- De native interface van VMware vShield biedt efficiënte toegang tot VM's, waardoor bronnen van individuele machines vrijkomen en compatibiliteit met andere VMware-technologieën is gegarandeerd
- De bronnen die vrijkomen door de anti-malwarefuncties en de definitiedatabase te concentreren op één virtuele appliance kunnen daardoor worden gebruikt om extra VM's te implementeren, waardoor de consolidatieratio toeneemt.
- As new VMs are booted up protection is provided instantly through the SVA, with no ‘instant on-gap' or the need for installation of any additional software.
- De immer beschikbare SVA van Kaspersky zorgt dat de definitiedatabase voortdurend wordt bijgewerkt en staat bovendien in verbinding met het Kaspersky Security Network (KSN). Dit is een wereldwijde infrastructuur die informatie verwerkt van miljoenen vrijwillige deelnemers en bescherming biedt tegen de meest recente dreigingen, zelfs nog voordat deze worden bestreden via de database-updates.
- Het probleem van 'stormen' is geëlimineerd, aangezien er maar één SVA hoeft te worden bijgewerkt. Deze SVA scant de VM's automatisch volgens een ingestelde planning waarbij een vooraf opgegeven maximum aantal threads wordt gebruikt.

Dankzij fundamentele netwerkbeveiligingsfuncties die worden geleverd door vCloud Networking and Security, kan de oplossing van Kaspersky inkomende aanvallen op VM's detecteren en schade voorkomen door de aanval te blokkeren met de Network Attack Blocker-technologie[1].

Helaas is de vShield-functionaliteit beperkt, omdat toegang tot beveiligde VM's alleen op niveau van het bestandssysteem wordt verleend. Dat bekent dat processen die plaatsvinden binnen het geheugen van de VM niet kunnen worden bewaakt en gecontroleerd door agentless anti-malware. Dit betekent ook dat andere beveiligingstechnologieën voor endpoints, zoals Application Control met dynamische whitelists (bedoeld om krachtige extra beveiligingslagen te verschaffen), niet kunnen worden geïmplementeerd.

Hierbij moet worden opgemerkt dat het agentless beveiligen van een virtuele infrastructuur momenteel alleen kan worden toegepast op het VMware-platform, aangezien vShield eigen technologie van VMware is.

Light Agent-benadering

Rekening houdend met de bovenstaande beperkingen biedt **Kaspersky Lab** een andersoortige oplossing voor virtualisatie, een benadering die het midden houdt tussen Agentless en Full Agent: **Kaspersky Security for Virtualization | Light Agent**.

Net als bij de Agentless-benadering bevinden de databases en de anti-malware-engine voor het scannen van bestanden zich op de SVA. Er is echter een verschil: er wordt een lichte residente module geïmplementeerd op elke VM die wordt beschermd.

Kaspersky Security for Virtualization | Light Agent wordt niet beperkt door de beveiligingsfuncties van de vShield-technologie, maar heeft rechtstreeks volledige toegang tot elke VM, waaronder alles wat er in het werkgeheugen gebeurt. Hierdoor kunnen alle geavanceerde technologieën van Kaspersky Lab worden ingezet om de gevirtualiseerde infrastructuur te verdedigen.

Belangrijke voordelen van Kaspersky Security for Virtualization | Light Agent zijn:

- Minder bronnenverbruik in vergelijking met een Full Agent-oplossing, doordat de engine en databases voor het scannen van het bestandssysteem op de speciale SVA staan.
- Ondersteuning voor de drie meest gebruikte virtualisatieplatformen: VMware, Microsoft Hyper-V en Citrix*
- Het hoogst mogelijke beschermingsniveau dankzij volledige toegang tot de VM-bronnen, waaronder het werkgeheugen.
- Er zijn extra proactieve beveiligingslagen beschikbaar, zoals HIPS met Automatic Exploit Prevention en Application Control met dynamische whitelists. De meest strikte beveiligingsscenario's, waaronder 'Default Deny', kunnen eenvoudig worden geïmplementeerd.
- Doordat de oplossing werd ontwikkeld met virtualisatie in het achterhoofd, werkt deze prima samen met de unieke functies van de virtuele omgeving, in plaats van deze tegen te werken.

Uiteraard zijn er ook nadelen. De Light Agent moet aanwezig zijn op elke nieuw geïmplementeerde VM. Dit proces kan eenvoudig worden geautomatiseerd door de Light Agent op te nemen in de vooraf gegenereerde VM-image. Door de aanwezigheid van de Light Agent heeft Kaspersky Security for Virtualization | Light Agent een iets grotere footprint in het geheugen dan de Agentless-applicatie. Hierbij moet wel worden opgemerkt dat de Light Agent onder bepaalde omstandigheden beter presteert dan de Agentless-applicatie met vShield.

Het is ook belangrijk om te onthouden dat het aantal ondersteunde hypervisors beperkt is tot de drie meest gebruikte platformen. Daarnaast is de Microsoft Windows-familie het enige gastbesturingssysteem dat zowel de Agentless- als de Light Agent-applicatie ondersteunt (ten tijde van het schrijven van dit document).

Maar dat betekent zeker niet dat u zich niet kunt verdedigen als u niet één van deze drie platformen gebruikt. Dan kunt u nog steeds de Full Agent-beveiligingsoplossing overwegen die is ontwikkeld door Kaspersky Lab.

Full Agent-benadering

Kaspersky Endpoint Security doet het meer dan behoorlijk in virtuele omgevingen, ondanks dat het een Full Agent-oplossing is. Hoewel Kaspersky Endpoint Security meer bronnen verbruikt dan Kaspersky Security for Virtualization kan deze oplossing ook in virtuele omgevingen worden toegepast. Het is ook mogelijk om een niet-standaardconfiguratie te beveiligen, bijvoorbeeld een aantal Linux-servers of Windows-gastsystemen op een exotische hypervisor.

De voordelen van het implementeren van Kaspersky Endpoint Security voor uw virtuele infrastructuur zijn:

- Ondersteuning voor de modernste besturingssystemen
- Bevat de meest uitgebreide set geavanceerde technologieën van Kaspersky Lab
- Vertrouwde beheerprincipes, hetzelfde als bij een fysieke machine
- De efficiëntie wordt bevestigd door Gartner, IDC en Forrester, drie toonaangevende adviesorganisaties, die het een van de beste platformen voor endpointbescherming noemen: een 'drievoudige bekroning'.

---

1 Voor het configureren van netwerkbescherming in KSV | Agentless moet een secundaire SVA worden geïmplementeerd

Tabel 1: Functievergelijking

Functie	Kaspersky Security for Virtualization | Agentless	Kaspersky Security for Virtualization | Light Agent	Kaspersky Endpoint Security for Business
Ondersteunde virtualisatieplatformen	VMware	VMware, Microsoft Hyper-V, Citrix	Alle, behalve besturingssysteemniveau[1]
Ondersteund gastbesturingssysteem	MS Windows	MS Windows	MS Windows, Mac OS X, Linux
Consolidatieratio op één host	* * *	* */* * *[2]	*
Gecentraliseerd beheer via Kaspersky Security Center	+	+	+
KSN-functionaliteit	+	+	+
Bescherming van nieuwe VM zonder extra installaties	+	+/-[3]	-
Anti-malware	* *	* * *	* * *
Firewall	-	+	+
Host-based Intrusion Prevention (HIPS)	-	+	+
Network Attack Blocker	+	+	+
Application Control met dynamische whitelists en ondersteuning voor Default Deny	-	+	+
Web Control	-	+	+
Device Control	-	+	+
Systems Management	-	+[4]	+[4]
Encryptie	-	-	+

Na al het saaie rekenwerk rijst de vraag dus weer: hoe kunt u maximale efficiëntie bewerkstelligen zonder uw bedrijf bloot te stellen aan cyberdreigingen? Er is een benadering die als uitgangspunt kan worden genomen en dat is **rolgebaseerde beveiliging.**

---

[1] – *Bij virtualisatie op besturingssysteemniveau, ook wel zonegebaseerde of containergebaseerde virtualisatie genoemd, wordt gebruikgemaakt van een mechanisme waarbij een groot aantal 'containers' met gebruikersruimte één besturingssysteemkernel delen. Parallels en Proxmox zijn voorbeelden van dergelijke platformen.*

[2] – *Is afhankelijk van hypervisor en type virtualisatie.*

[3] – *Voor niet-persistente VM's is onmiddellijke bescherming beschikbaar nadat de Light Agent in de image van de VM wordt opgenomen. Voor persistente VM's moet de beheerder de Light Agent handmatig implementeren.*

[4] – *Technologie voor vulnerability-beoordeling en patchbeheer zorgt voor een hoog bronnenverbruik en wordt daarom afgeraden voor virtuele omgevingen, ook al zijn deze technologieën tot op zekere hoogte mogelijk in Kaspersky Security for Virtualization | Light Agent.*

Verdedig uzelf tegen aanvallen; een rolgebaseerde benadering van beveiliging.

Elke cyberdreiging die uw fysieke endpoints aanvalt kan zich ook richten tegen uw virtuele infrastructuur. Voordat een aanval kan plaatsvinden zal de aanvaller echter eerst uw netwerkbeveiliging moeten omzeilen. Als een cybercrimineel bijvoorbeeld een bedrijfs-pc wil infecteren, moet hij eerst de werknemer naar een schadelijke website lokken om een vulnerability in de browser van het slachtoffer te kunnen misbruiken. Maar als de crimineel bijvoorbeeld een databaseserver wil besmetten die zich diep binnen de IT-infrastructuur van het bedrijf bevindt en die misschien niet eens een internetverbinding heeft, zal hij een andere ingang moeten zoeken. Dus als u er zeker van bent dat de enige mogelijke dreigingen gericht zijn op het niveau van het bestandssysteem, dat de desbetreffende gegevens op zichzelf geen al te hoge waarde hebben of als u een VDI met strenge beleidsregels en zonder internettoegang gebruikt, dan kunt u kiezen voor een agentless oplossing met als voordelen onmiddellijke bescherming en geen hiaat bij inschakeling.

Tabel 2: Rolgebaseerde beveiliging

Functie	Externe toegang	Waarde gegevens*	Waarde service**	Ext. omstandigheden	Oplossing (waarom bepaalde oplossing moet worden gebruikt)
Back-end databaseservers	Nee	Laag tot middelhoog	Middelhoog tot hoog	Regelmatige back-ups	KSV | Agentless (korte gebruiksduur gegevens, minder infectiehaarden)
Front-end webservers	Ja	Laag	Hoog	Hebben vertrouwensrelaties met meerdere back-ends	KSV | Light Agent (Blootgesteld aan gevaren van openbare toegang, na een succesvolle aanval is misbruik is mogelijk)
VDI met beperkt gebruiksdoel of gevirtualiseerde applicatie	Nee	Middelhoog tot hoog	Middelhoog	Zeer beperkt, geen installatie van apps, geen gebruik van verwisselbare storage	KSV | Agentless (voorspelbare omgeving, minder infectiehaarden)
VDI als vervanger van desktopcomputers	Ja	Middelgrote bedrijven	Middelgrote bedrijven	Persoonlijke verwisselbare storage in gebruik, gebruikers met installatierechten	KSV | Light Agent (De behoefte aan betere beveiliging is groter dan de behoefte aan snellere respons, meer infectiehaarden vanwege blootstelling aan openbaar internet)
Webservers voor bedrijfsintranet	Ja	Laag tot middelhoog	Laag tot middelhoog	*Externe toegang door uitsluitend geautoriseerde gebruikers met hardwaretokens	KSV | Agentless (Lage bedrijfswaarde van gegevens, zeer beperkte blootstelling aan openbaar internet)
Infrastructuur voor verwerking van klantgegevens	Ja	Hoog	Hoog	Behoefte aan stabiele, onveranderlijke omgeving; Application Control met Default Deny aanbevolen	KSV | Light Agent (Door behoefte aan regelnaleving zijn extra beschermingslagen absoluut noodzakelijk.)
Testinfrastructuur voor webontwikkelaars	Ja	Laag tot middelhoog	Middelhoog	Linux-gebaseerde hypervisor en heterogene gast-VM's	KESB voor Linux, KESB voor Windows (constant vernieuwde gegevens met korte gebruiksduur, verscheidenheid aan besturingssystemen)

De bovenstaande tabel bevat enkele voorbeelden die een algemeen inzicht bieden in rolgebaseerde verdediging, maar is niet bedoeld als directe aanbeveling voor de vermelde rollen en moet ook niet als zodanig worden gebruikt. Elk gebruiksgeval is uniek. Er zijn altijd meer omstandigheden waarmee rekening moet worden gehouden dan kunnen worden samengevat in één tabel. Om het concept echter te verduidelijken, zullen we de classificatie voor Waarde gegevens en Waarde service nader toelichten:

- **Gegevens met lage waarde:** deze gegevens bevatten meestal geen identiteitsgegevens, waardevolle persoonlijke of commerciële informatie, staatsgeheimen, hebben een korte gebruiksduur en worden continu ververst. Het verlies of openbaar worden van deze gegevens leidt niet tot significante commerciële verliezen of reputatieschade. Een goed voorbeeld hiervan is een database waarin tijdelijk overgangsgegevens worden opgeslagen.
- **Gegevens met middelhoge waarde:** deze gegevens kunnen enige persoonlijke of commerciële informatie bevatten, maar geen gegevens die rechtstreeks verband houden met financiën of persoonlijk welzijn. Deze gegevens bevatten geen geheime informatie. Het verlies ervan kan het bedrijf enige financiële schade toebrengen. Het openbaar worden van de gegevens kan leiden tot merkbare financiële gevolgen en reputatieschade voor het bedrijf. Voorbeeld: klantgegevens van een webwinkel.
- **Gegevens met hoge waarde:** kunnen vertrouwelijke persoonlijke en/of financiële informatie of commerciële geheimen bevatten die belangrijk zijn voor de concurrentiepositie van het bedrijf. Deze kunnen ook geheime informatie bevatten. Het verlies van deze gegevens kan leiden tot aanzienlijke commerciële schade en reputatieschade. Het openbaar worden van de gegevens kan leiden tot ernstige financiële gevolgen, waaronder boetes en rechtszaken, en tot onherstelbare reputatieschade. Voorbeeld: blauwdrukken van cruciale infrastructuur of vertrouwelijke correspondentie tussen directieleden.
- **Service met lage waarde:** geen gevolgen voor derden en een snel herstel is niet echt belangrijk. Uitval van de service heeft weinig of geen financiële gevolgen. De kans op reputatieschade is zeer gering. Voorbeeld: de informatieportal van een bedrijf.
- **Service met middelhoge waarde:** uitval van de service kan gevolgen hebben voor derden. Het verlies van dergelijke gegevens kan merkbare financiële gevolgen hebben. Ook reputatieschade is mogelijk, en dit hangt rechtstreeks samen met het sociale belang van de service: hoe bekender en populairder de service (of een product dat ervan afhankelijk is), hoe groter de reputatieschade is. De gegevens zijn mogelijk onderdeel van een overheidsinfrastructuur, maar hebben nauwelijks invloed op het nationale welzijn. Snel herstel is van essentieel belang. Voorbeeld: een VDI-infrastructuur van een systeemintegrator die een desktopvervangende omgeving aanbiedt.
- **Service met hoge waarde:** uitval van de service heeft vrijwel zeker gevolgen voor derden. De service is een essentieel element van de bedrijfsactiviteiten en dat geldt mogelijk ook voor derden. Invloed op het nationale welzijn is mogelijk. Reputatieschade is uiterst pijnlijk en mogelijk onherstelbaar. Herstel is essentieel: als snel herstel niet mogelijk blijkt, kan dat verstrekkende gevolgen hebben. Voorbeeld: de infrastructuur van een videobewakingssysteem bij een overheidsinstelling.

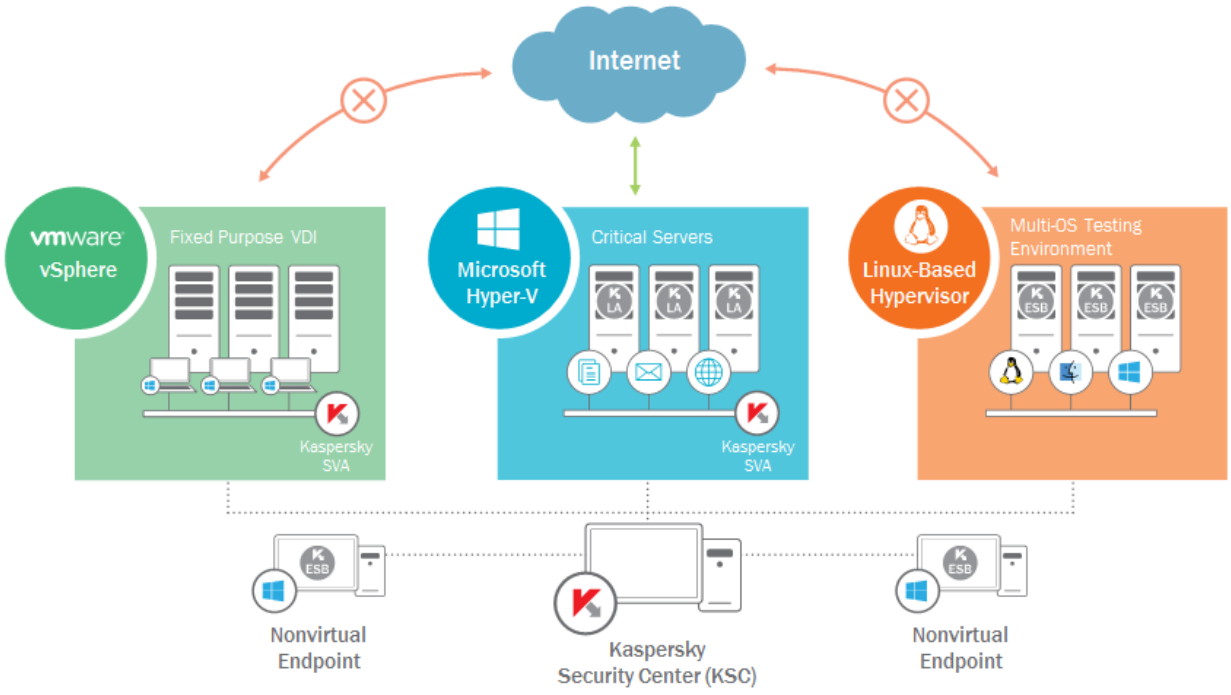
Omdat u uw eigen infrastructuur het beste kent, bent u de aangewezen persoon om te beslissen hoe u uw beveiliging het beste kunt inrichten. De hier vermelde richtlijnen zijn enkel bedoeld als richtlijn voor het nemen van een besluit. Maar het is zeker mogelijk om een efficiënter bronnenverbruik en geldbesparing voor uw bedrijf te verwezenlijken, en tegelijkertijd uw virtuele infrastructuur te beschermen. Vergeet niet om eerst de basisbeveiligingsinstellingen van uw IT-netwerk te controleren en waar nodig aan te passen voordat u een gespecialiseerde beveiligingsoplossing gaat implementeren. Een goed beheerd netwerk betekent minder zwakke plekken waarvan criminelen misbruik kunnen maken en minder schade als het toch fout gaat.

Efficiëntie betekent integriteit

Efficiënt bronnenverbruik is mooi, maar zonder effectieve controle hebt u er niets aan. Het staat u uiteraard vrij om een agentless oplossing van de ene leverancier te implementeren voor uw back-ends, een Light Agent-oplossing voor uw VDI van een andere leverancier en ook nog een Application Control-oplossing van een derde leverancier. Het gevolg is dan wel dat u drie beheerconsoles hebt, drie sets beleidsregels die u moet configureren en onderhouden en excessief updateverkeer op uw gegevensverbinding. Het is veel beter als u al uw oplossingen bij dezelfde leverancier afneemt en kunt beschikken over één overzichtelijke beheerconsole. Alle beveiligingsproducten van Kaspersky zijn ontwikkeld om centraal te worden beheerd en aangestuurd via Kaspersky Security Center (KSC). Hierdoor kunt u al uw gevirtualiseerde bedrijfsmiddelen beheren via dezelfde console als uw fysieke endpointbeveiliging.

Een ander voordeel is gecentraliseerd updaten. Het is niet nodig om dezelfde set updates te downloaden voor elke SVA op elke hypervisor. De updates worden automatisch toegepast nadat deze zijn gedownload naar de KSC-storage.

Nog een onderscheidend element van de oplossingen van Kaspersky Lab is de beschikbaarheid voor verschillende virtualisatieplatformen. U kunt dus een goed beveiligde omgeving met meerdere hypervisors inrichten en toch optimaal profiteren van één geïntegreerde beheeromgeving in KSC.



Afbeelding 1: ook een omgeving met meerdere hypervisors kan solide en efficiënt worden beschermd

Zo kunt u bijvoorbeeld uw Active Directory-kernsystemen (domeincontrollers, DNS, enz.) hosten op virtuele servers met Microsoft Hyper-V, een VDI met Citrix implementeren en daaraan nog een paar databaseservers toevoegen die draaien op VMware ESXi. U kunt ook, zoals hierboven afgebeeld, een gemengde omgeving inrichten met meerdere hypervisorplatformen in combinatie met fysieke endpoints.

Om de beste balans tussen prestaties en beveiliging te bewerkstelligen met het oog op optimale consolidatieratio's:

- Kan de geïsoleerde VDI met vast gebruiksdoel worden beschermd met KSV | Agentless
- Moet de bedrijfskritische serverinfrastructuur met waardevolle gegevens worden beschermd door de robuuste beveiligingslagen van KSV | Light Agent
- Kan de testomgeving met een Linux-hypervisor en een groot aantal gastbesturingssystemen en fysieke endpoints het beste worden afgeschermd met Kaspersky Endpoint Security.

In elk geval bieden de producten van Kaspersky Lab u de beste bescherming die de branche te bieden heeft. U kunt kiezen tussen de eenvoudige implementatie en kostenvoordelen van KSV | Agentless, de robuuste bescherming van KSV | Light Agent of een willekeurige combinatie daarvan binnen één IT-infrastructuur.

Kaspersky Lab kan klanten virtualisatieoplossingen met Agentless, Light Agent en Agent bieden, waardoor we onze klanten volstrekt objectieve aanbevelingen kunnen doen. We hoeven geen specifieke technologie te promoten, maar kunnen voor elke specifieke klantomgeving de beste optie of combinatie van opties aanreiken. En omdat al onze oplossingen zijn gebaseerd op dezelfde krachtige anti-malware-engine en zijn ontwikkeld als onderdeel van één geïntegreerd beveiligingsplatform, weten we zeker dat uw virtuele systeem veilig zal zijn, welke oplossing u ook kiest.