KASPERSKY lab

AAN HET ROER VAN DATACEN-TERBEVEILIGING: U BENT AAN ZET

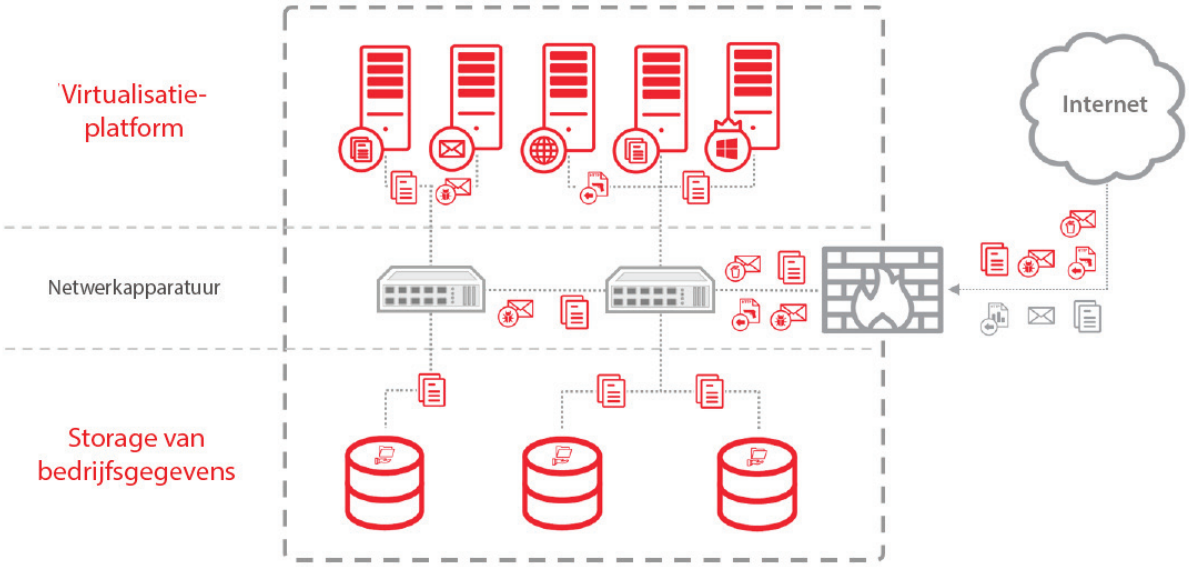
INLEIDING

Een datacenter omvat een veelheid aan complexe taken, waarvan de beveiliging er slechts één is. Maar de beveiliging van virtuele omgevingen en data storage in het bijzonder is van cruciaal belang voor het moderne datacenter. De beveiliging van die twee gebieden is altijd een uitdaging. Pakt u die uitdaging niet goed aan, dan kan dat vervelende gevolgen hebben, voor uw klanten en voor het datacenter zelf. Helaas zijn sommige problemen niet altijd duidelijk, of worden ze gewoon genegeerd tot het te laat is. Laten we deze problemen eens onder de loep nemen en nagaan hoe we ze kunnen voorkomen.

VIRTUALISATIEBEVEILIGING: FOUTEN EN DE GEVOLGEN ERVAN

Virtualisatie van verschillende bedrijfsmiddelen is sterk in opkomst. Dit zorgt voor een optimaal gebruik van bronnen, meer flexibiliteit en meer schaalbaarheid. En veel scenario's waarbij virtuele infrastructuren een rol spelen, lenen zich ervoor om aan de zorg van een datacenter te worden toevertrouwd. Door de uiteenlopende activiteiten die datacenters ondernemen, krijgt de beveiliging van gehoste bedrijfsmiddelen echter te vaak geen aandacht.

Daar zijn diverse redenen voor te noemen. Klanten voelen zich meer op hun gemak met hun eigen traditionele manier van beveiligen, of ze zijn terughoudend om het beveiligingsbeheer over te dragen een derde partij. Het gebeurt soms ook dat providers zelf liever niet de verantwoordelijkheid voor de beveiliging van gehoste bedrijfsmiddelen op zich nemen.



Een datacenter biedt klanten verschillende soorten bronnen die allemaal beveiligd moeten worden.

De gevolgen van een dergelijke houding kunnen zuur zijn. “Dingen doen omdat we het altijd zo hebben gedaan” kan resulteren in een chaotische mix aan beveiligingsoplossingen van verschillende klanten, zonder oog voor virtualisatie, die allemaal op dezelfde host worden uitgevoerd of, erger nog, helemaal geen beveiligingsoplossing. Die afwezigheid kan worden verklaard door verrassend hardnekkige mythen dat 'virtuele omgevingen inherent veilig zijn' en dat 'malware niet op virtuele machines voorkomt'.

De waarheid is uiteraard het omgekeerde: VM's (virtuele machines) zijn vatbaar voor de meeste gangbare aanvalsvormen en kennen zelfs vaak extra vulnerabilities voor exploitatie. VDI's (Virtual Desktop Infrastructures) die vaak op dezelfde manier worden gebruikt als hun fysieke tegenhangers (zoals toegang tot internet en alle gevaren vandien), zijn met name vatbaar voor infecties.
Binnen de kortste keren kunnen onbeschermde vulnerabilities leiden tot een malware-uitbraak, die niet alleen de aanvankelijk aangevallen klant raakt, maar ook anderen met bedrijfsmiddelen op dezelfde host. Een plotselinge toename in het gebruik van bronnen na een uitbraak kan tot vertragingen leiden, en kan zelfs de hele host laten vastlopen: uiterst vervelend voor niet-geïnfecteerde klanten.

Eén specifieke gevirtualiseerde infrastructuur in het datacenter kan zelfs als springplank dienen voor verdere aanvallen, waarbij hele IP-adresreeksen worden uitgesloten. Dat trekt de aandacht van de autoriteiten en tast de probleemloze werking van het datacenter danig aan.

De installatie van beveiligingsoplossingen op gevirtualiseerde endpoints zonder oog voor virtualisatie kan echter voor eigen problemen zorgen.

Deze omvatten:

- Overmatig gebruik van bronnen, waarbij elke beschermde machine complete sets gerepliceerde componenten bevat: een scansysteem, een lokale definitiedatabase, een Host-based Intrusion Prevention System etc. En als cloudgebaseerde feeds met informatie over dreigingen worden gebruikt, is er voor elke feed een eigen stukje bandbreedte nodig.

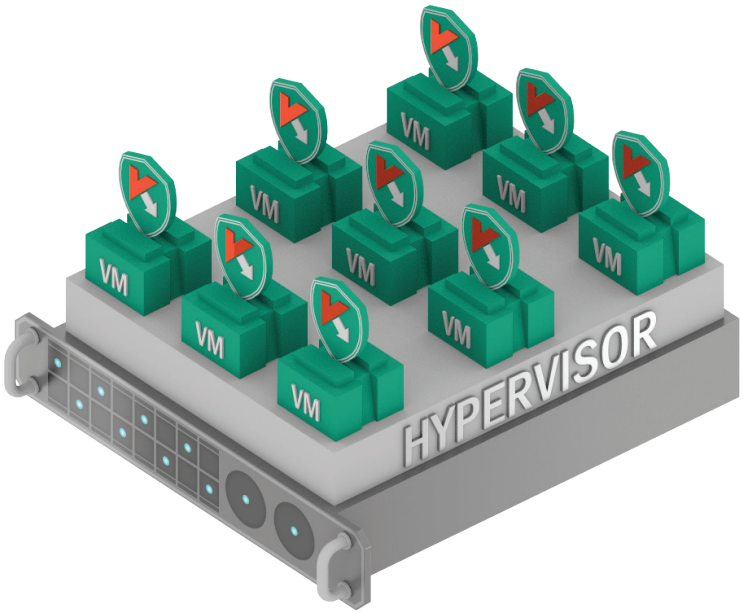
- Onvoorspelbare pieken in het gebruik van bronnen, 'stormen' genoemd, die worden veroorzaakt door de simultane uitvoering van soortgelijke taken, zoals updates of scans van het bestandssysteem, op meerdere VM's. Dit kan tot behoorlijke vertragingen leiden of zelfs tot DoS-gebeurtenissen (Denial of Service) voor de gehele hostmachine.

- Paniekaanvallen: malware-uitbraken zorgen vaak voor paniekreacties zoals ongeplande scans, intensievere scans etc. De resulterende afname in prestaties kan alle gehoste VM's op dezelfde server hinderen.

- 'Beveiligingsrisico's bij inschakelen': sommige VM's kunnen 'slapen' tot hun services nodig zijn. In die status kunnen ze niet worden bijgewerkt (zoals patching van vulnerabilities en updates van de beveiligingsoplossing). Direct na het opstarten blijft de machine kwetsbaar tot deze volledig is bijgewerkt. Er is dus genoeg tijd om een infectie op te lopen.

- Incompatibiliteit. Hoewel VM's in veel opzichten op hun fysieke tegenhangers lijken, zijn er ook enkele verschillen. Beveiligingsoplossingen zonder oog voor virtualisatie zijn niet geschikt voor, bijvoorbeeld, dynamisch toegewezen virtuele storages of VM-migratie. Dat kan leiden tot kleine of grotere fouten.

Het is van cruciaal belang om in te zien dat de serviceprovider uiteindelijk verantwoordelijk zal worden gehouden voor de hier genoemde gevolgen. Het feit dat u geen controle over gehoste bronnen hebt, telt niet als verweer. Dat is des te meer zo omdat er WEL manieren zijn om zaken onder uw efficiënte controle te brengen in een gevirtualiseerde omgeving.



1. Veroorzaakt 'updatestormen'
2. Veroorzaakt 'scanstormen'
3. 'Risico's bij inschakeling'
4. Overmatig gebruik van bronnen
5. Verlaagt VM-dichtheid
6. Geen beveiliging voor netwerkbronnen

Het gebruik van bescherming zonder oog voor virtualisatie zorgt voor meerdere problemen, om te beginnen bij het inefficiënte gebruik van bronnen.

Het antwoord is het gebruik van specialistische beveiligingsoplossingen, die met name rekening houden met virtualisatie.

GEBRUIK BESCHERMING DIE BIJ U PAST

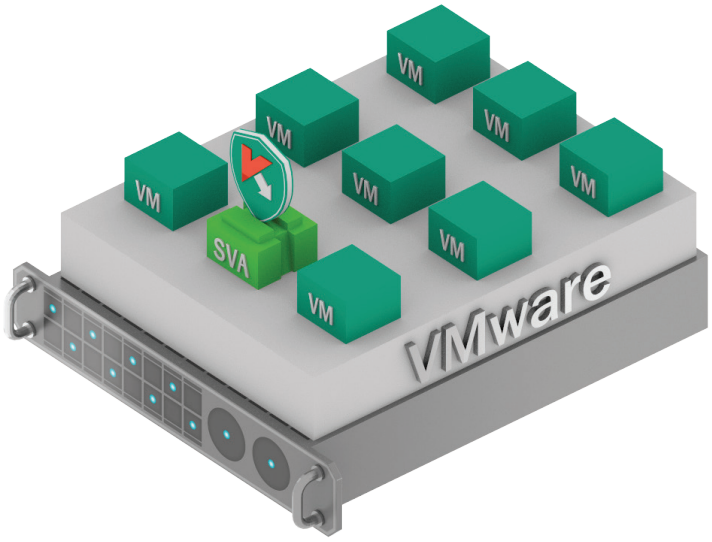
Kaspersky Security for Virtualization is ontwikkeld met alle kennis van virtuele infrastructuren en past op natuurlijke wijze in dergelijke omgevingen. Problemen als gevolg van inadequate, inefficiënte of ongepaste oplossingen worden zo vermeden.

Ten eerste wordt de redundantie van identieke componenten op elke VM geëlimineerd. Een speciale VM die **Security Virtual Appliance (SVA)** heet, bevat zowel het scansysteem als de beveiligingsdatabase op een centrale plaats. Elke VM onder dezelfde hypervisor wordt zo beschermd. Deze wordt voortdurend bijgewerkt en gebruikt slimme plantechnieken om het scannen te beheren en zo stormen te vermijden.

Uiteraard moet de SVA elke beschermde VM kunnen bereiken. Kaspersky Security for Virtualization biedt daartoe twee verschillende manieren:

Agentless

Deze optie werkt alleen in VMware-gebaseerde omgevingen. Zoals de naam al aangeeft, hoeft er geen softwareagent op de VM te worden geïnstalleerd. Er wordt gebruikgemaakt van de native vShield-technologie. Met deze Agentless-optie **wordt elke VM automatisch beschermd**, vanaf het moment van ingebruikname, terwijl een extra SVA **Intrusion Prevention System (IPS)**-functionaliteit voor het netwerk biedt.



Agentless-oplossing biedt directe bescherming zonder iets op VM te hoeven installeren

Deze Agentless-aanpak is de perfecte keuze voor de bescherming van klanten die huiverig zijn om vreemde software in hun machines toe te laten, of die alleen een strikt gedefinieerde set apps uitvoeren. En in situaties waarin klanten HELEMAAL geen beveiligingsoplossing willen gebruiken, is dit wellicht de enige manier om grote beveiligingshiaten te vermijden.

Er zijn echter een paar overwegingen die aandacht behoeven. Agentless-technologie staat niet toe dat de beveiligingsoplossing processen in het geheugen van VM's controleert: alleen vShield-technologie biedt toegang tot bestandssystemen van machines, wat de effectiviteit van de bescherming tegen geavanceerde malware (zoals bodiless variaties) beperkt.

Ook is het niet mogelijk om aanvullende proactieve beveiligingslagen te implementeren zoals Application, Device of Web Controls. Voor sommige scenario's, zoals de VDS's (Virtual Desktop Infrastructures) die steeds vaker fysieke werkstations vervangen, bevelen we dan ook een andere optie aan die Kaspersky Security for Virtualization biedt: bescherming met Light Agents.

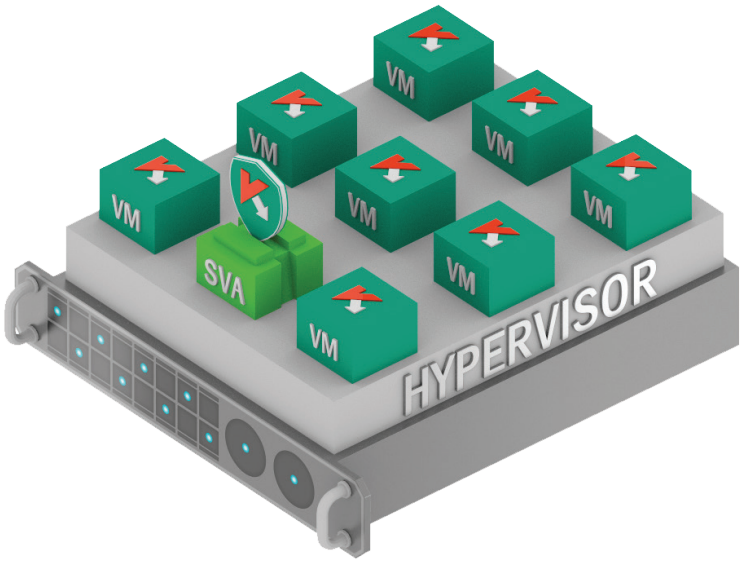
Light agent

Anders dan bij Agentless-beveiliging is deze optie niet gebaseerd op een **platformafhankelijke tussenlaag**. Deze optie kan dus werken met een breder bereik van hypervisors en met ondersteuning voor Microsoft Hyper-V en Citrix. Dat is mogelijk dankzij de toepassing van een **lichte softwareagent** in de beschermde VM. De aanwezigheid van deze agents zorgt er niet alleen voor dat beschermde machines worden bereikt door het anti-malwaresysteem van de SVA, maar biedt ook veel meer beschermende technologieën. Het beveiligingsniveau wordt zo opgekrikt tot het **equivalent van een complete endpointbeveiligingsoplossing**, zoals Kaspersky Endpoint Security for Business.

Kaspersky Security for Virtualization | Light Agent biedt onder meer de volgende opties:

- Controle over processen in het geheugen van VM's op basis van geavanceerde gedragsmechanismen
- Beperking van exploits dankzij Automatic Exploit Prevention-technologie
- Anti-virus op het web met cloudondersteunde anti-phishing
- Een complete set beveiligingsbeheertools, die de set toegestane applicaties, webbronnen of zelfs externe apparaten op individuele VM's expliciet kunnen definiëren.
- Netwerkbescherming verbeterd met blokkeermechanismen tegen netwerkaanvallen en geavanceerde firewalls en controles zorgen voor beveiliging op helpniveau voor elke virtuele-machinebewerking binnen gevirtualiseerde netwerken.

Ondanks al die kracht blijft de agent zeer licht. De SVA handelt nog steeds updates en scans af, zodat redundanties worden geëlimineerd en agent-based activiteiten op de VM op een veilig minimum blijven.

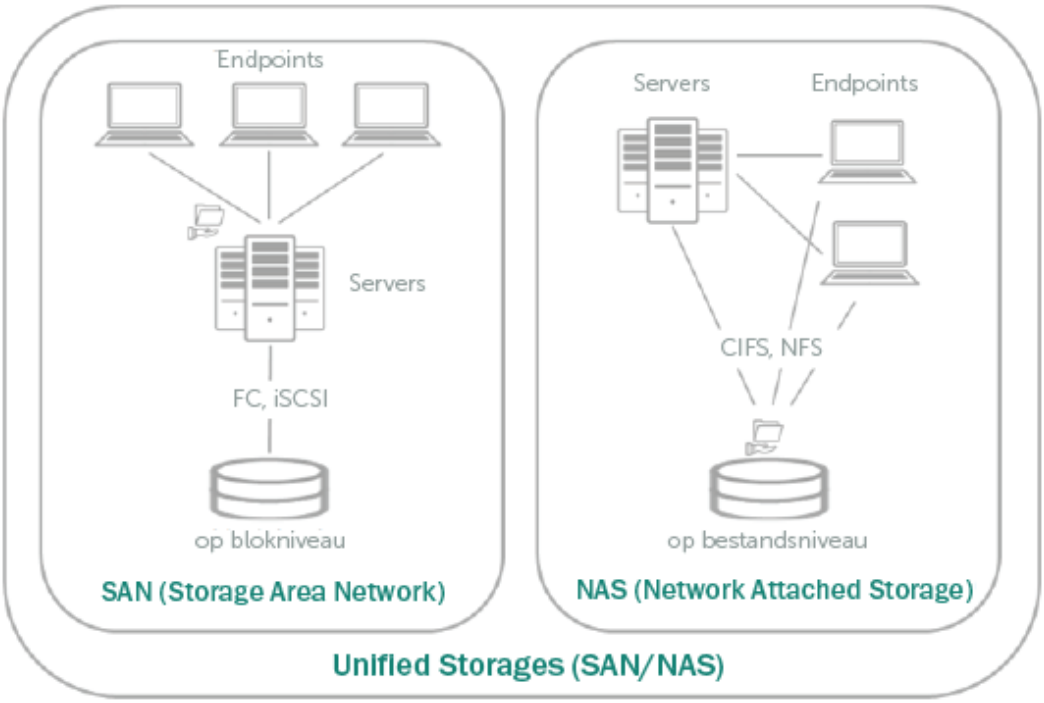


Een oplossing met Light Agents bieden geavanceerde bescherming op basis van lichte apps die op VM's inwerken. Deze apps zijn vooraf op VM-images te installeren.

Voor scenario's met meer risico's en bredere potentiële aanvalsoppervlakken (zoals gevirtualiseerde desktops met volledige internetmogelijkheden), is een dergelijke meerlaagse bescherming een must – en niet alleen vanwege de grotere kansen op een aanval. Gevirtualiseerde netwerken zijn veel efficiënter, waardoor een infectie zich razendsnel kan verspreiden en aanvallers binnen een mum van tijd de controle krijgen over volledige infrastructuren die slecht zijn beschermd. Aan de andere kant vormt een goed beschermde virtuele infrastructuur een minder aantrekkelijk doel, zelfs voor doelgerichte aanvallers op zoek naar gemakkelijke prooien.

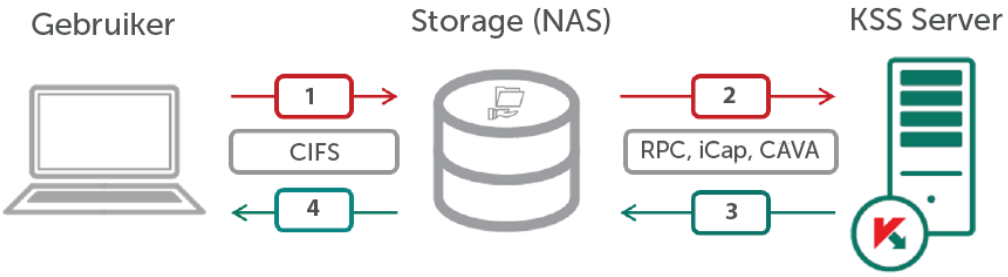
BEVEILIGING VAN DATA STORAGE – GEVIRTUALISEERD OF NIET

Bij de overweging van datacenterbeveiliging moet men data storage niet over het hoofd zien. Er worden grote hoeveelheden gegevens opgeslagen, bijgewerkt en gedeeld. Deze vormen een potentiële bron van gevaar voor honderden gebruikers als ook maar één van deze gebruikers onoplettend of zelfs kwaadwillend is. Het is ook goed om te bedenken dat gebruikers zich buiten de beschermde omgeving kunnen bevinden. Het datacenter heeft absoluut geen invloed op, of zelfs maar informatie over, hun beveiligingsstatus. Speciale maatregelen zijn dan ook nodig om verschillende soorten data storage te beveiligen, vooral als ze niet allemaal zijn gevirtualiseerd en beschermd door een virtualisatiespecifieke beveiligingsoplossing.



Verschillende soorten storage hebben allemaal bescherming nodig

Storage Area Networks (SAN's) zijn vrij eenvoudig te beschermen (aangezien ze alleen via servers toegankelijk zijn). De beveiliging van **Network-Attached Storages (NAS)**, waar netwerkgebruikers direct toegang toe hebben, is complexer.



De bescherming van NAS is gecompliceerder dan SAN

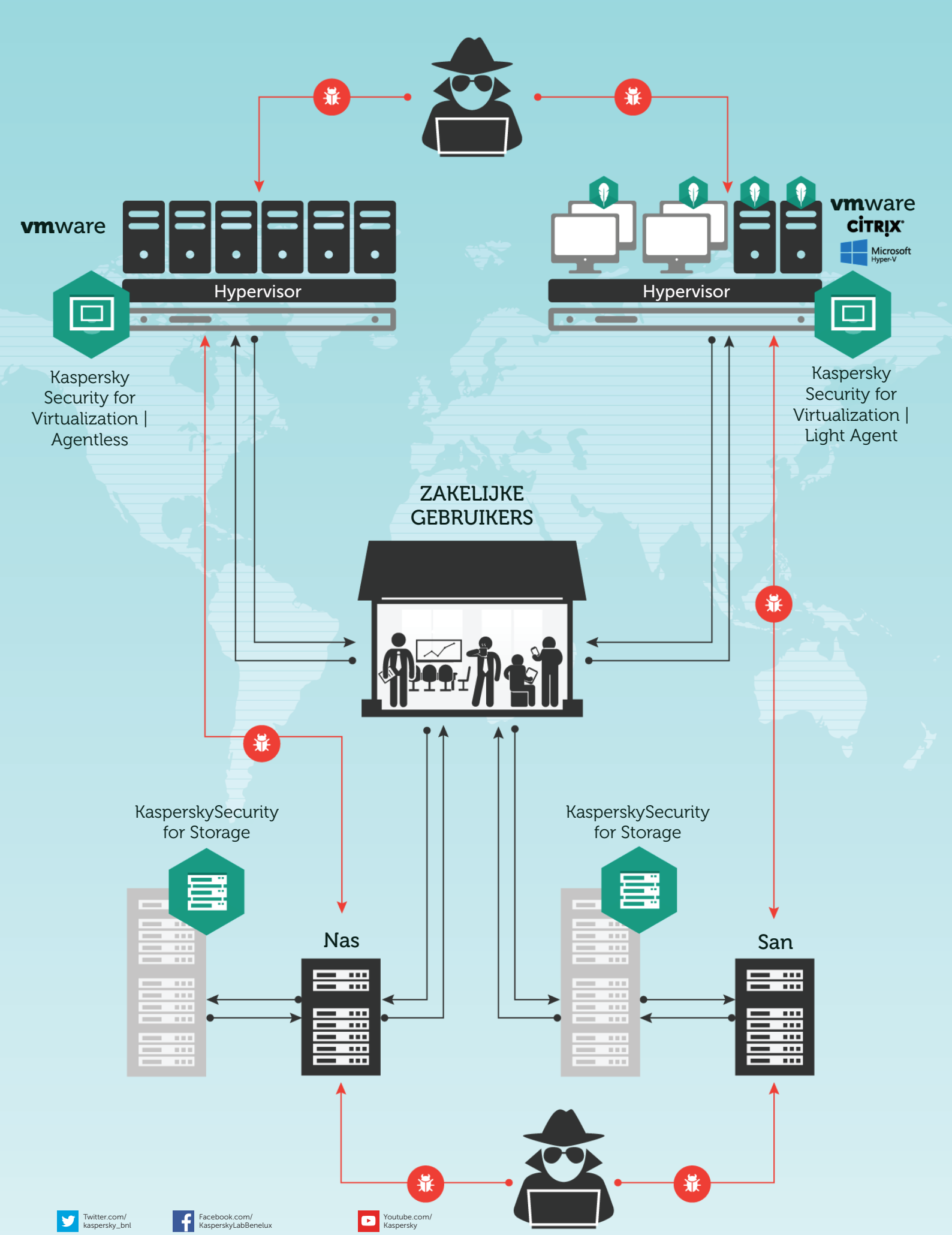
Gelukkig zijn er specialistische beveiligingsoplossingen die bescherming voor beide systemen kunnen bieden. Een goed voorbeeld is Kaspersky Security for Storage. SAN-bronnen worden beveiligd zoals gewone bestandssystemen, maar elk object dat wordt verzonden naar – of opgevraagd bij – NAS-gebaseerde data storage wordt eerst gecontroleerd door de oplossing van Kaspersky Lab. De oplossing bepaalt dan of de NAS toestemming geeft of weigert om de gewenste actie uit te voeren. Voor de afhandeling van intensievere gegevensstromen kunnen meerdere instanties van de oplossing worden geïmplementeerd, waarbij de NAS de werklast zelf verdeelt.

EÉN CONSOLE DIE ALLES REGELT

Met steeds meer en steeds geavanceerdere moderne cyberaanvallen is een goed overzicht van de gehele infrastructuur van belang voor iedereen die de beveiliging van het datacenter regelt. Alleen zo kunnen dreigingen tijdig worden gesignaleerd en onschadelijk gemaakt.
En op dat punt bieden oplossingen van Kaspersky Lab nog een voordeel: alle beveiliging wordt bewaakt en beheerd via één flexibele, gecentraliseerde console - Kaspersky Security Center. En optionele rolgebaseerde toegang betekent dat u uw klanten de gelegenheid kunt bieden om desgewenst hun eigen beveiligingsstatus te beheren, zonder de algehele beveiliging van het datacenter in gevaar te brengen.

CONCLUSIE

Of u nu te maken hebt met gevirtualiseerde of fysieke bedrijfsmiddelen, de Security Solution for Data Centers van Kaspersky Lab (onderdeel van ons Enterprise Security Platform) biedt een handige manier om IT-beveiliging om te vormen tot een aantrekkelijke – en winstgevende – optie als onderdeel van uw aanbod van datacenterservices. Maar één ding is absoluut duidelijk: u moet de beveiliging van uw datacenter zelf kunnen bepalen om komende stormen te overleven.



Twitter.com/ kaspersky_bnl

Facebook.com/ KasperskyLabBenelux

Youtube.com/ Kaspersky

Kaspersky Lab
kaspersky.nl

Alles over internetbeveiliging:
www.securelist.com

Zoek een partner bij u in de buurt:
kaspersky.nl/partners

KASPERSKY lab