KASPERSKY SECURITY FOR VIRTUALIZATION EN VMWARE NSX

HOOGWAARDIGE BEVEILIGING VOOR SOFTWAREGEDEFINIEERDE DATACENTERS

Gegevens zijn een van de belangrijkste peilers in uw bedrijf. Dus hoe en waar die gegevens worden opgeslagen, verwerkt en verzonden is van essentieel belang, niet alleen om een betere concurrentiepositie te verkrijgen, maar ook om de operationele efficiëntie en bedrijfscontinuïteit te garanderen.

Er bestaan veel uitstekende oplossingen voor het verwerken en opslaan van gegevens en voor het gebruik van netwerken. Maar met name netwerkoplossingen zijn in veel gevallen complex, inflexibel en vaak gebonden aan en beperkt tot het hardwareplatform waarop ze zijn ontwikkeld. Dit belemmert de flexibiliteit van uw datacenter en de mogelijkheid om aan snel veranderende bedrijfsbehoeften te voldoen.

VMware® en Kaspersky Lab pakken deze problemen samen aan met een gezamenlijke oplossing die is gebouwd rond een zeer efficiënt softwaregedefinieerd datacenter. Deze oplossing beschikt over geavanceerde beveiligingsmogelijkheden voor een hoog niveau van bescherming tegen interne en externe dreigingen.

INGEBOUWDE VMWARE NSX-SERVICES	
Gedistribueerde firewall	Virtuele netwerken (VXLAN)
Controle van serveractiviteiten	VPN (IPSec, SSL L2VPN)
KASPERSKY SECURITY FOR VIRTUALIZATION	
Anti-malware	Inbraakdetectie/-preventie (IDS/IPS) voor virtuele netwerken
Geautomatiseerde beveiliging	Op beleid gebaseerde integratie
Integratie van beveiligingstags	Volledig scannen van de infrastructuur, zelfs voor uitgeschakelde VM's

Kaspersky Security for Virtualization Agentless is speciaal ontworpen voor de beveiliging van softwaregedefinieerde datacenters op basis van VMware vSphere met NSX-technologieën. Onze beveiligingsoplossing biedt geavanceerde beveiligingsmogelijkheden met vrijwel geen effect op platformefficiëntie. Zo kunt u profiteren van een toonaangevende anti-malwareoplossing met behoud van hoge consolidatieratio's.

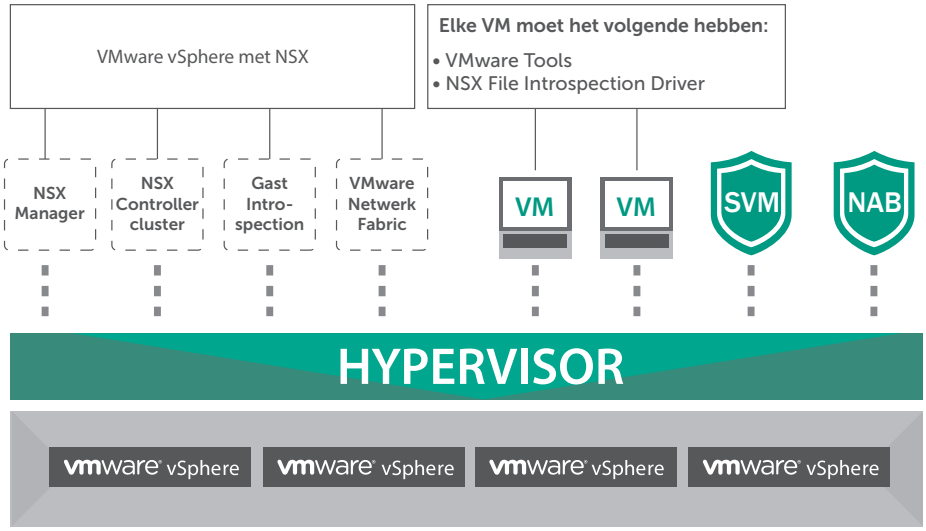
vmware PARTNER TECHNOLOGY ALLIANCE
vmware READY NETWORKING AND SECURITY
NUTANIX READY
VBLOCK READY
VCE VALIDATION READY

KASPERSKY lab

HOE PLATFORMINTEGRATIE WERKT

VMware NSX® reproduceert het netwerk van uw datacenter met een softwaregedefinieerd model, zodat u met verschillende pools netwerkbronnen kunt werken en binnen enkele seconden dynamisch uw gehele netwerktopologie kunt maken of kunt herconfigureren op basis van een 'zero trust'-beveiligingsmethode.

Door de naadloze integratie tussen het VMware NSX-platform en Kaspersky Security for Virtualization worden alle VM's (virtuele machines) en het gevirtualiseerde netwerk automatisch beveiligd tegen de meest geavanceerde dreigingen. Zonder dat er op de VM's een beveiligingsagent hoeft te worden geïnstalleerd, wordt er continue, alomvattende bescherming geleverd zonder gevolgen voor uw gevirtualiseerde platformbronnen.



BEVEILIGING VIRTUELE MACHINE
- Interne integratie met VMware NSX
- Ondersteuning voor NSX en vShield Endpoint
- Lage belasting van systeembronnen
- Scant in- en uitgeschakelde machines

NETWERKAANVALBLOKKER
- Krachtige beveiliging voor netwerken
- Controle van webverkeer door het scannen van URL's
- Heuristische analyse om applicaties te beschermen
- Directe bescherming voor de hele infrastructuur

Interne interactie tussen uw virtualisatieplatform en de bijbehorende beveiligingsoplossing betekent dat uw softwaregedefinieerde datacenter in real-time kan reageren op beveiligingsincidenten binnen uw gehele infrastructuur.

SPECIFIEK ONTWORPEN VOOR VMWARE NSX-BEVEILIGING

- De meest bekroonde anti-malware-engine herkent en blokkeert bekende, onbekende en zelfs zero-day cyberdreigingen.
- Door geautomatiseerde implementatie voor VMware NSX verschijnt de SVM (Security Virtual Machine) automatisch op de hypervisor, volgens op de eisen van de beschermde VM's op die host.
- Integratie van beveiligingsbeleid betekent dat elke VM precies de beveiligingsmogelijkheden krijgt die in uw bedrijfsbeleid zijn gedefinieerd voor de specifieke functie van de VM.
- Door integratie met NSX-beveiligingstags kan uw softwaregedefinieerde datacenter in real-time reageren op beveiligingsincidenten en indien nodig de gehele virtuele infrastructuur automatisch herconfigureren.
- Proactieve bescherming tegen geavanceerde dreigingen door het gebruik van het cloudgebaseerde Security Network.
- Dankzij gelijktijdige ondersteuning voor zowel NSX als vShield Endpoint zijn uw IT- en beveiligingsstrategieën volledig afgestemd op de behoeften van uw bedrijf.

GEAUTOMATISEERDE BEVEILIGING EN BEWAKING

- Door de infrastructuur volledig te scannen worden alle VM's beschermd, zowel online als offline, voor een nog betere beveiliging voor uw gehele infrastructuur.
- Routinematig scannen van alle VM's kan vooraf worden gepland op gedetailleerd niveau, zodat beveiligingstaken aan uw behoeften kunnen worden aangepast.
- Door zelfbescherming en geavanceerde SNMP-gebaseerde bewaking zijn SVM's altijd actief en kunnen ze uitgebreide informatie aan bewakingstools van derden leveren voor extra controle.
- Geavanceerde beveiliging wordt nooit onderbroken, zelfs niet als een werklast van de ene naar de andere host wordt verplaatst. De eigen functies van VMware vMotion en Disaster Recovery worden volledig ondersteund.
- Door interne integratie met VMware vCenter Server en NSX Manager is uw beveiligingslaag altijd op de hoogte van wijzigingen in de infrastructuur.

DE JUISTE BALANS TUSSEN BESCHERMING EN PRESTATIES

- Dankzij bekroonde anti-malwarebeveiliging die is ontworpen voor virtualisatie kunnen taken voor het scannen van bestanden voor meer efficiëntie worden verplaatst van de afzonderlijke VM's naar een speciale SVM.
- Indringingsdetectie- en -preventie (IDS/IPS) voor virtuele netwerken werkt in een agentless modus waarbij uw volledige gevirtualiseerde infrastructuur wordt beveiligd tegen netwerkdreigingen.
- Met optimalisatie op basis van cache wordt gegarandeerd dat onlangs gescande bestanden niet opnieuw worden gescand tijdens een routinematige scan.
- Onze beveiligingsoplossing gaat efficiënt om met bronnen, waardoor de IT-prestaties verbeteren en de computerinfrastructuur minder wordt belast.

SUPERIEURE BETROUWBAARHEID EN BEHEER

- Met één gemeenschappelijke beheerconsole voor virtuele, fysieke en mobiele apparaten kunt u een consistent beveiligingsbeleid voor al uw IT-systemen afdwingen.
- Implementatie zonder downtime: u hoeft VM's niet opnieuw op te starten en de hostserver niet in de onderhoudsmodus te zetten.
- Door intelligente planning van scantaken en automatisering vermijdt u pieken in het verbruik van hypervisorbronnen en blijft de algehele efficiency van het platform gehandhaafd.
- Dankzij uitgebreide rapportage en bewaking kunt u de beveiliging in uw hele organisatie gemakkelijker beheren en controleren.

Het resultaat is een flexibele, gevirtualiseerde bedrijfsomgeving met uitstekende prestaties en toonaangevende beveiliging.

OPTIMALE BEVEILIGING VOOR UW SOFTWAREGEDEFINIEERDE DATACENTER

Virtuele en fysieke infrastructuren hebben te maken met dezelfde dreigingen. Cybercriminelen maken geen onderscheid. U kunt zich niet veroorloven om concessies te doen aan de beveiliging. En ook niet aan de prestaties.

1 CYBERDREIGINGEN BEHOREN NU TOT HET VERLEDEN

Kaspersky Security for Virtualization is gebaseerd op de meest bekroonde beveiligingsengine op de markt en helpt u binnen uw hele gevirtualiseerde IT-landschap zelfs de meest geavanceerde bedreigingen en beveiligingslekken het hoofd te bieden. Onze beveiligingsoplossing is speciaal ontworpen om gebruik te maken van de technologische voordelen van virtualisatieplatformen en zo krachtige beveiliging te bieden met optimale snelheid en een efficiënt gebruik van rekenkracht.

2 ONTWIKKELD EN GEOPTIMALISEERD VOOR VMWARE NSX

Systeemeigen integratie van onze agentless oplossing met het VMware NSX-platform betekent dat uw virtuele infrastructuur nog efficiënter en winstgevender is geworden. Vanaf nu werken uw VMware vSphere met NSX-infrastructuur en de bijbehorende beveiligingslagen samen om nieuwe niveaus van automatisering en beleidsgestuurde beveiliging te bieden, waardoor de bedrijfsvoering dankzij de geautomatiseerde bescherming met gedetailleerde beveiligingsmogelijkheden die snel kunnen worden geleverd middels de integratie van beveiligingsbeleid en beveiligingstags.

3 ZICHTBAARHEID EN BEHEERBAARHEID OP BEDRIJFSNIVEAU

Dankzij één geïntegreerde beheerconsole kan uw IT-team de beveiliging van al uw VM's centraal beheren, samen met de beveiligingsapplicaties van Kaspersky Lab die u op fysieke infrastructuur en mobiele apparaten uitvoert. Met Kaspersky Lab kan uw team makkelijker hybride omgevingen beheren (waarin virtuele, fysieke en mobiele platforms zijn gecombineerd), zodat u virtualisatieprojecten in uw eigen tempo kunt implementeren met minder druk op de IT-bronnen en minder ruimte voor menselijke fouten.

Kaspersky Security for Virtualization biedt de meest geavanceerde beveiligingsmogelijkheden voor hybride bedrijfsomgevingen op basis van het VMware NSX-platform en het hoogst mogelijke efficiencyniveau, aangezien de oplossing de systeemprestaties niet beïnvloedt. De virtualisatiebewuste architectuur van Kaspersky Lab's beveiligingsoplossing biedt een uitgebreide toolset van beschermende technologieën die efficiënt kunnen worden geïntegreerd en op core-niveau samenwerken met de IT-infrastructuur. Hybride infrastructuren hebben extra voordelen doordat ze samenwerken met Kaspersky Security for Virtualization.

Meer informatie vindt u op www.kaspersky.com/data-center-security

KASPERSKY lab