Security for Data Centers

KASPERSKY SECURITY FOR VIRTUALISATION

Superieure, flexibele en efficiënte bescherming voor virtuele servers en VDI

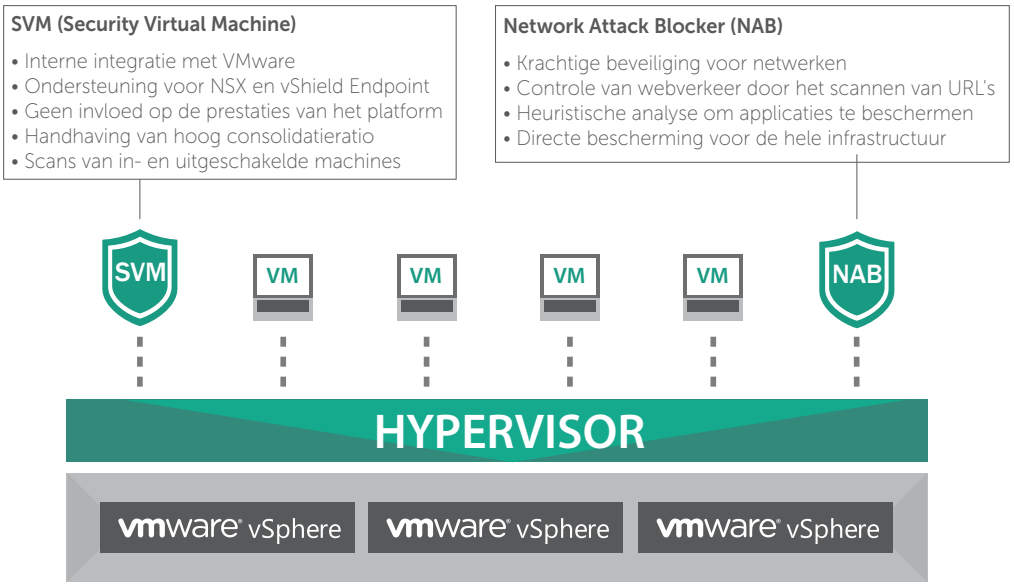
Nu steeds meer bedrijven profiteren van de voordelen van softwaregedefinieerde datacenters, is de behoefte aan uitstekende bescherming zonder in te boeten op productiviteit nog nooit zo groot geweest.

Dit is precies wat Kaspersky Security for Virtualization levert: uitstekende meerlaagse, gedetailleerde en krachtige bescherming voor VDI en virtuele servers en omgevingen, verbeterd door nauwe integratie met de populairste virtualisatieplatforms en -technologieën, zoals VMware vSphere met NSX, Microsoft Hyper-V, Citrix XenServer en KVM, evenals VMware Horizon en Citrix XenDesktop.

Met Kaspersky Securtiy for Virtualization, een oplossing met agentless en light agent opties, herdefiniëren we de interactie tussen uw softwaregedefinieerde datacenter en de beveiligingsoplossing hiervan waarbij het datacenter en de oplossing elkaar versterken en nog slimmer, sneller en efficiënter worden.

Agentless integratie met VMware NSX

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



- **Meest bekroonde anti-malware-engine** is verbeterd doordat de indringingsdetectie en -preventie (IDS/IPS) voor virtuele netwerken bekende, onbekende en zelfs zero-day cyberdreigingen herkent en blokkeert.
- **Volledig geautomatiseerde implementatie** van gespecialiseerde beveiligingsapplicaties op basis van het beveiligingsbeleid dat op elke VM op de hypervisorhost wordt toegepast.
- **Integratie met NSX-beveiligingsbeleid** waardoor elke VM exacte, gedetailleerde beveiligingsmogelijkheden krijgt en u uw infrastructuur onbeperkt kunt uitbreiden.
- **Integratie met NSX-beveiligingstags** waardoor uw softwaregedefinieerde datacenter in real-time kan reageren op beveiligingsincidenten en indien nodig de gehele virtuele infrastructuur automatisch kan herconfigureren.
- **Proactieve bescherming tegen geavanceerde dreigingen** door gebruik van het cloudgebaseerde Security Network.

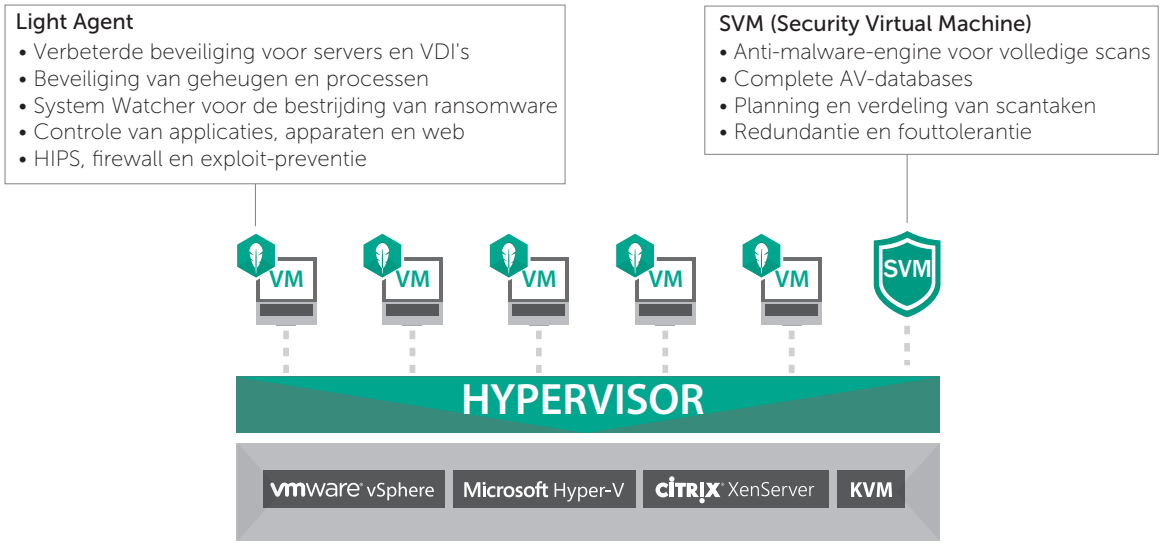
vmware PARTNER TECHNOLOGY ALLIANCE
vmware READY NETWORKING AND SECURITY
CITRIX READY
NUTANIX READY
VBLOCK READY
VCE VALIDATION READY

Light agent biedt meer beveiligingslagen

Terwijl agentless integratie met VMware NSX meer automatisering biedt, hebben uw bedrijfskritische virtuele servers en desktops hogere beschermingsniveaus nodig omdat activiteiten op bestandsniveau en in de netwerkinfrastructuur niet de enige mogelijke vectoren voor cyberaanvallen zijn. U hebt meer beveiliging nodig.

Kaspersky Security for Virtualization Light Agent biedt één oplossing voor de beveiliging van zowel virtuele servers als VDI. Omdat er ondersteuning wordt geboden voor de populairste platforms, inclusief VMware vSphere, Citrix XenServer, Microsoft Hyper-V en KVM, is deze oplossing ideaal voor hybride softwaregedefinieerde datacenters. Een krachtige maar light beveiligingsagent ondersteunt toonaangevende VDI-platforms zoals Citrix XenDesktop en VMware Horizon, en verbetert de beveiliging aanzienlijk terwijl de prestaties van elke VM op niveau blijven.

HOE HET WERKT EN WAT HET DOET



* Amerikaans patent nr 9009836 en nr 9088618

Een Security Virtual Machine (SVM) op elke host scant alle VM's centraal, terwijl met een krachtige light agent op elke VM geavanceerde beveiligingsfuncties mogelijk zijn, waaronder controls voor applicaties, apparaten en web, anti-malwarebeveiliging voor e-mail en webverkeer, evenals geavanceerde heuristiek. Pieken in het bronnenverbruik worden verminderd door Intelligent Scan Task Orchestration, waarmee wachtrijen worden geautomatiseerd door scantaken op meerdere beveiligde VM's samen te voegen en hier prioriteiten aan toe te kennen.

- **System Watcher**-technologie maakt gebruik van Behaviour Stream Signatures voor het behoud van de consistentie van elke VDI en de bescherming tegen crypto-lockers en ransomware.
- **Application Startup and Privilege Control,** inclusief Default Deny, controleert de activiteiten van de gebruiker zodat op een beschermde VM alleen vertrouwde applicaties kunnen worden gestart.
- **Network Attack Blocker ondersteund met het moderne Host-Based Intrusion Prevention System** beschermt de gevirtualiseerde omgeving tegen netwerkaanvallen.
- **URL-beveiliging** beschermt elke VM tegen malware en verdachte internetbronnen die schadelijk kunnen zijn of die niet voldoen aan het beveiligingsbeleid.
- Met **bescherming van e-mail en webverkeer** is alle communicatie binnen uw bedrijfsomgeving veilig en komt binnen zonder malware.
- **Device Control** biedt gegarandeerd veilige toegang tot gevirtualiseerde apparaten die zijn aangesloten op een virtuele desktop.

Welke gevirtualiseerde platform(s) u ook gebruikt, Kaspersky Security for Virtualization biedt met zijn perfect ontwikkelde technologieën en unieke architectuur meer beveiligingsmogelijkheden. VMware vSphere met NSX, Microsoft Hyper-V, Citrix XenServer en KVM worden ondersteund vanuit één beveiligingsoplossing. Ongeacht uw platformconfiguratie en hybridisatie, en ongeacht of het gaat om interne of externe systemen, al het beveiligingsbeheer wordt uitgevoerd via één geïntegreerde console en de volledige efficiency van de systemen blijft gehandhaafd.

Kaspersky Security for Virtualization Light Agent en Agentless Twee beveiligingsbenaderingen in één oplossing bieden krachtige bescherming in combinatie met efficiënte prestaties voor uw virtuele omgeving.

Ga voor meer informatie over Kaspersky Security for Virtualization naar www.kaspersky.com/enterprise

KSV/January17/Global