KASPERSKY lab

LIGHT AGENT OF AGENTLESS

Een functieoverzicht voor Kaspersky Security for Virtualisation

www.kaspersky.nl

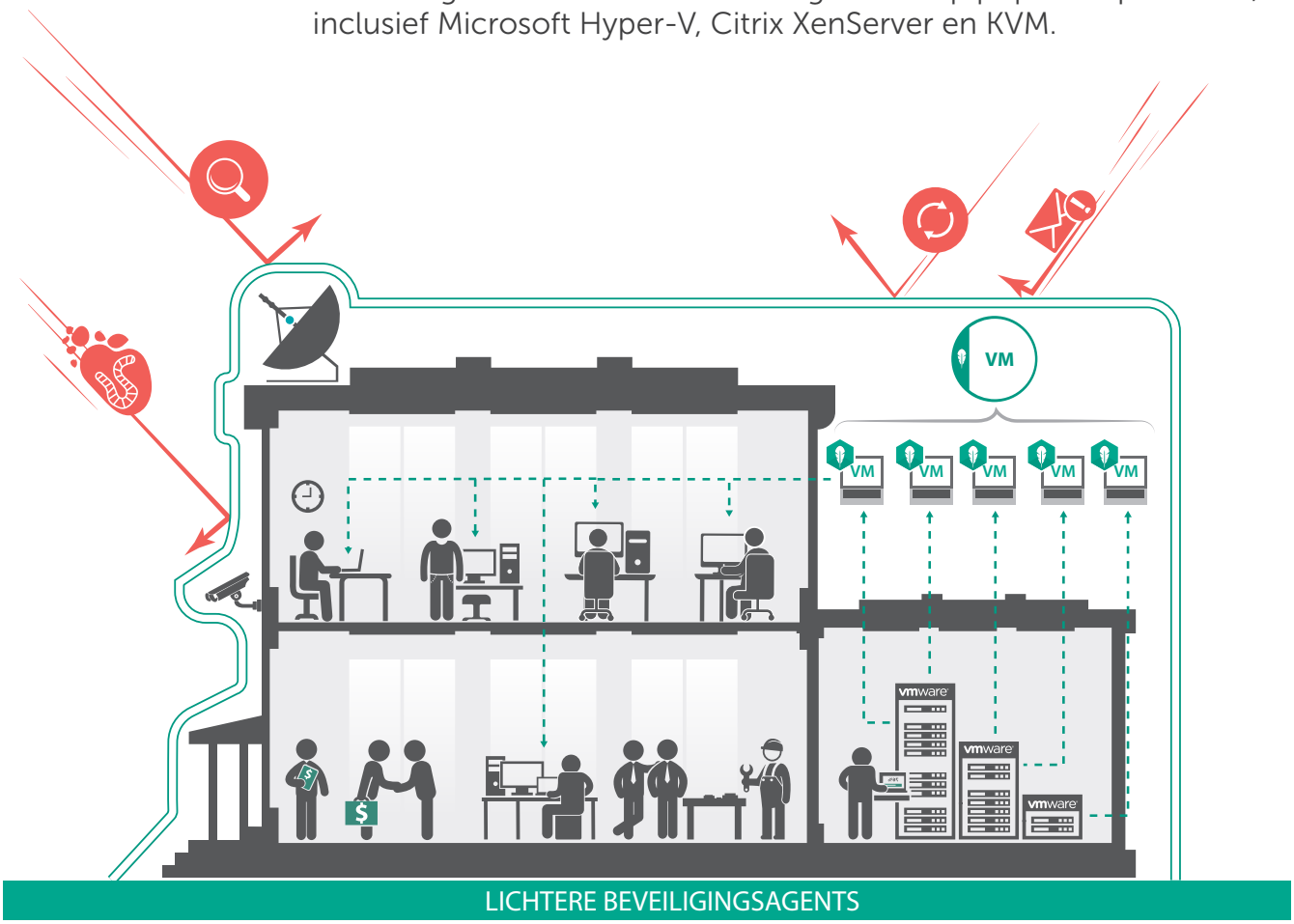
Omdat virtualisatie steeds meer wordt gebruikt, spreekt het voor zich dat er ook behoefte aan passende beveiligingsoplossingen is. Hoewel virtuele systemen net zo vatbaar zijn voor cyberaanvallen als fysieke systemen, hebben zij unieke functies waarvoor speciale aandacht nodig is bij het beoordelen van beveiligingsoplossingen.

Bedrijven kunnen gebruikmaken van dezelfde beveiligingssoftware voor het beschermen van zowel hun fysieke systemen als virtuele machines. Standaardoplossingen die niet specifiek zijn ontworpen voor virtuele omgevingen bieden een goed beveiligingsniveau, maar kunnen toch problemen met zich meebrengen, zoals:

1. **Excessief verbruik van systeembronnen** door de replicatie van definitiedatabases en actieve anti-malware-engines op elke beveiligde VM (virtuele machine).
2. **'Stormen'**: gelijktijdige database-updates en/of anti-malwarescans op alle VM's waardoor het verbruik van systeembronnen enorm toeneemt, met als gevolg een drastische verslechtering van de prestaties en mogelijk een DoS (denial of service). Bij pogingen om het probleem te beperken door deze processen te plannen, ontstaan er zogenaamde 'vulnerability windows': de tijd waarin de VM kwetsbaar is voor aanvallen door uitgestelde malwarescans.
3. **'Hiaten bij inschakeling'.** Definitiedatabases kunnen niet worden bijgewerkt op inactieve VM's. Hierdoor is de VM kwetsbaar voor aanvallen vanaf het opstarten van de machine totdat de update is voltooid.
4. **Incompatibiliteit.** Omdat standaardoplossingen niet zijn ontwikkeld voor virtualisatiespecifieke functies, zoals de migratie van VM's of niet-persistente storage, kan het gebruik van dergelijke oplossingen leiden tot instabiliteit of zelfs het vastlopen van het systeem.

Marktleider VMware zag in dat het belangrijk was virtuele systemen te beveiligen en besefte dat er bij virtualisatie sprake is van unieke functies. Met dit in gedachten werd de vShield Endpoint-technologie ontwikkeld, een specifieke defensieve laag voor het vSphere-virtualisatieplatform. Deze laag zorgt voor een geïntegreerde beveiligingsruimte voor oplossingen van derden die intern wordt geïntegreerd met VMware API's zoals vShield Endpoint en NSX Guest Introspection. Deze beveiligingsruimte bevat ook alle gevirtualiseerde assets en is eenvoudig en efficiënt toegankelijk voor adequaat ontworpen beveiligingsoplossingen. Per host is er slechts één Security Virtual Machine (SVM, een gespecialiseerde virtuele machine met een anti-malwarescan-engine en definitiedatabases) nodig , waardoor afzonderlijke VM's niet met deze belasting te maken krijgen en het bronnengebruik aanzienlijk wordt verminderd. Het grootste voordeel van deze aanpak voor grote ondernemingen is een probleemloze interne integratie met het VMware-ecosysteem.

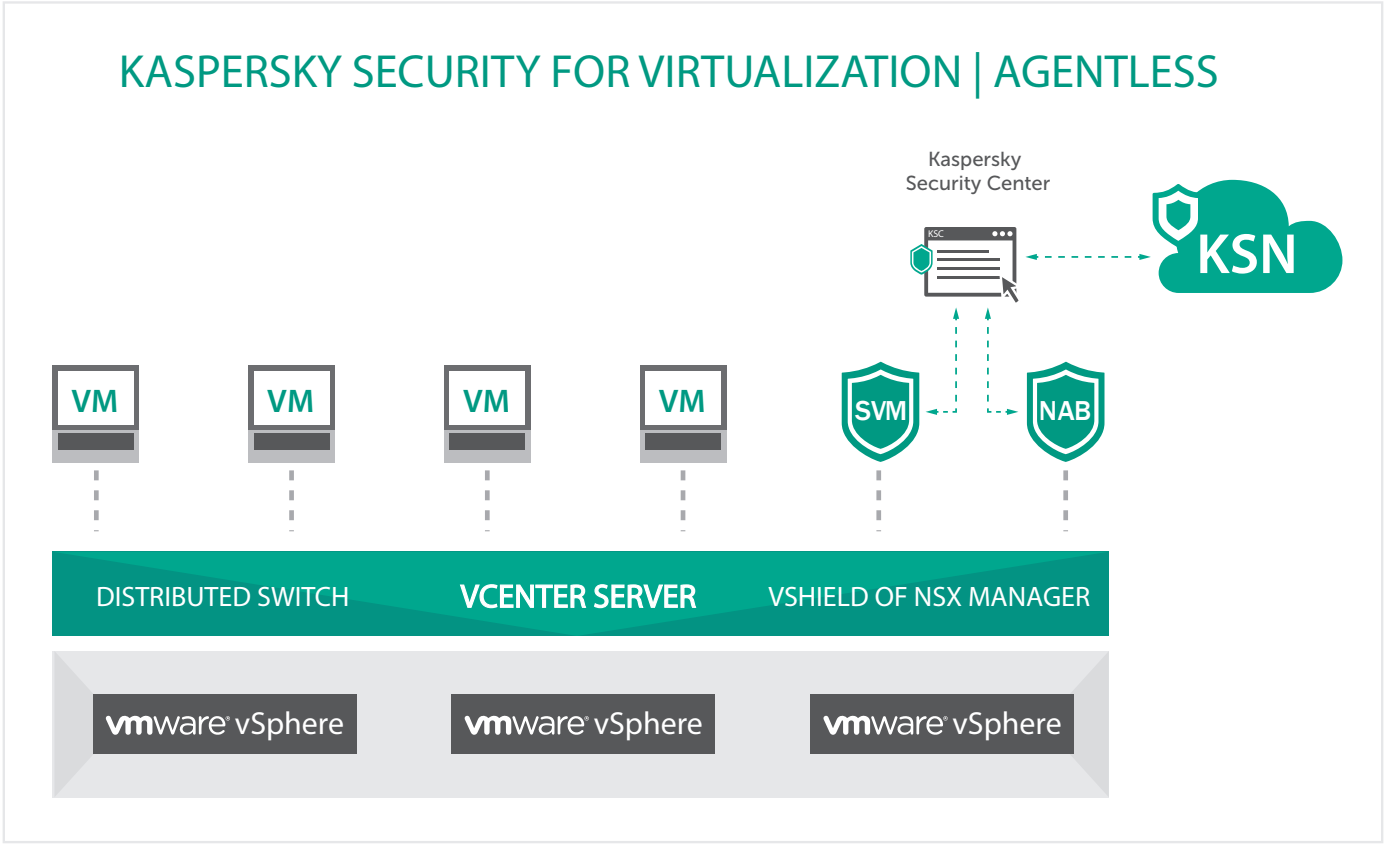
Een andere benadering is een API-onafhankelijke of eigenlijk een virtualisatieplatformonafhankelijke oplossing die gebruikmaakt van een lichtgewicht agent die is geoptimaliseerd om te werken binnen het besturingssysteem van elke VM die wordt beschermd. Bij de 'light agent'-technologie wordt de engine voor het scannen van bestanden en databases nog steeds centraal op de SVM gehouden, maar het bronnenverbruik is aanzienlijk lager dan bij een traditionele, volledige agent-based oplossing. De oplossing ligt tussen agentless en traditionele volledig agent-based oplossingen wat betreft het bronnenverbruik, maar is niet gebonden aan of beperkt door VMware-technologieën en kan ook worden gebruikt op populaire platforms, inclusief Microsoft Hyper-V, Citrix XenServer en KVM.



KASPERSKY SECURITY FOR VIRTUALIZATION | AGENTLESS

Kaspersky Security for Virtualization | Agentless is speciaal ontworpen om gebruik te maken van alle voordelen van de vShield Endpoint-technologie. De kant-en-klare Security Virtual Machine (SVM) werkt met Kaspersky Lab's bekroonde anti-malware-engine en profiteert daardoor van de uitstekende detectieresultaten van deze engine. Ondersteuning voor de Kaspersky Security Network-cloudservice zorgt voor de snelst mogelijke reactietijd en, belangrijker, detecteert nieuwe malwaredreigingen in slechts 0,02 seconden. Hierdoor kunt u met Kaspersky Security for Virtualization uw gevirtualiseerde omgeving zelfs beveiligen tegen zero-day dreigingen.

VMware NSX-omgevingen profiteren van de integratie tussen Kaspersky Security for Virtualization | Agentless en VMware's eigen NSX Guest Introspection, zodat u uw infrastructuur zonder beperkingen kunt uitbreiden terwijl uw beveiligingsoplossing naadloos de topologie en veranderingen in de infrastructuur volgt.



Voor geavanceerde netwerkbeveiliging kan een tweede SVA worden gebruikt om de functionaliteit van Kaspersky Network Attack Blocker te leveren, in nauwe integratie met VMware's NSX-platform alsmede met de vCloud Networking & Security-component.

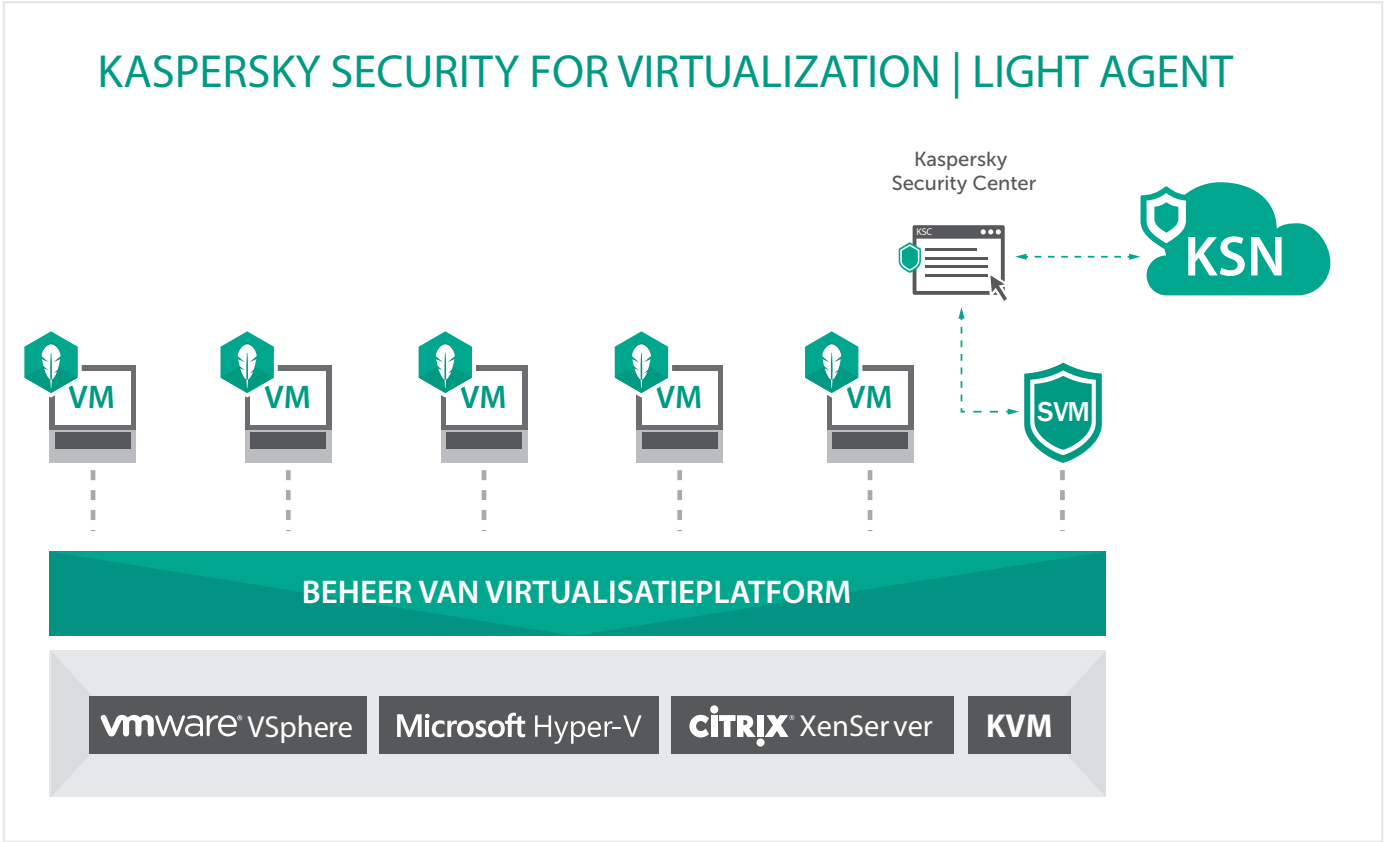
De agentless benadering kent enkele beperkingen. Ten eerste is VMware vSphere het enige virtualisatieplatform met een tussenliggende beveiligingslaag: NSX of vShield Endpoint. Voor andere virtualisatieplatforms moet de beveiligingsoplossing een bepaalde vorm van een agent binnen het gastbesturingssysteem van afzonderlijke VM's installeren voor het scannen van bestanden op machineniveau. Ten tweede bieden de eigen technologieën zoals vShield Endpoint en NSX Guest Introspection als gevolg van het ontwerp van VMware geen toegang tot de interne processen van de VM, applicaties of webverkeer, of tot gevirtualiseerde apparaten. De beveiliging van de infrastructuur is beperkt tot scannen op bestandsniveau, waardoor de oplossing aanzienlijk minder diepe bescherming tegen geavanceerde malware op het niveau van afzonderlijke VM's kan leveren.

KASPERSKY SECURITY FOR VIRTUALIZATION | LIGHT AGENT

Bij een 'light agent'-aanpak zijn deze beperkingen opgelost. Bij deze applicatie wordt de engine voor het scannen van bestanden en databases nog steeds centraal op de SVM gehouden, maar is het bronnenverbruik aanzienlijk lager dan bij traditionele volledige agent-based oplossingen. De light agent op elke VM biedt toegang tot het geheugen van afzonderlijke machines, applicaties en interne processen, evenals tot het webverkeer en gevirtualiseerde apparaten. Door deze toegang kunnen geavanceerde beveiligingstechnieken worden geïmplementeerd op het niveau van de VM, terwijl de algehele efficiëntie en prestaties van het virtualisatieplatform behouden blijven.

Kaspersky Security for Virtualization | Light Agent is speciaal ontworpen voor virtuele omgevingen en ondersteunt de populairste platforms: Citrix XenServer, Microsoft Hyper-V, VMware en sinds kort KVM.

In gevirtualiseerde serveromgevingen profiteren gebruikers van Kaspersky Security for Virtualization | Light Agent van waardevolle



technologieën zoals HIPS (Host-Based Intrusion Prevention System) en een eigen firewall ter bescherming tegen netwerkaanvallen. Voor VDI-omgevingen is de beveiliging uitgebreid met geavanceerde functies voor netwerkbeveiliging en een volledige set endpoint-controls, zodat u niet alleen uw systemen tegen malware beschermt, maar ook het gebruik van niet-vertrouwde applicaties, apparaten of webbronnen beperkt. Door de architectuur van de oplossing is het aanvalsoppervlak aanzienlijk kleiner, waardoor er minder computerbronnen nodig zijn. Een krachtige, meerlaagse, defensieve omgeving waar geavanceerde malware en zelfs zero-day dreigingen worden tegengegaan, wordt aangevuld door de AEP-technologie (Automatic Exploit Prevention).

Een 'light agent'-aanpak betekent dat u uw virtuele omgeving, inclusief virtuele servers en VDI, kunt beveiligen zonder noemenswaardige gevolgen voor de prestaties van de hypervisor. U kunt uw systemen en gevoelige bedrijfsgegevens dus volledig beveiligen zonder dat dit gevolgen heeft voor de machinedichtheid en de kwaliteit van de gebruikerservaring.

BEVEILIGINGSTECHNOLOGIEËN VAN KASPERSKY VERSUS DREIGINGEN VOOR UW VIRTUELE INFRASTRUCTUUR

VM's zijn misschien wel nog kwetsbaarder dan hun fysieke tegenhangers omdat de verspreiding van een besmetting in de razendsnelle gevirtualiseerde netwerken desastreus kan zijn. Het is dus belangrijk de zwakke punten in de beveiliging van uw virtuele infrastructuur te kennen en een efficiënte beveiligingsoplossing met specifieke bescherming tegen geavanceerde dreigingen te implementeren. Hieronder bespreken we mogelijke dreigingen voor virtuele systemen en de technologieën die worden gebruikt om de dreigingen te bestrijden.

Uitvoerbare bestanden van malware

Ongeacht of het gaat om verraderlijke bijlagen bij e-mails, besmette leisureware of een tijdelijk uitvoerbaar bestand dat is gemaakt door malware, anti-malwarebeveiliging is essentieel om deze basisdreigingen onschadelijk te kunnen maken. Onze krachtige engine voor de bestrijding van malware is het kernoderdeel van zowel onze Agentless- als Light Agent-versie van Kaspersky Security for Virtualization, hoewel er verschillende middelen worden gebruikt om bij de bestanden van de beveiligde VM te komen.

Een andere manier om te voorkomen dat malware-agents schade aan uw gevirtualiseerde systemen aanrichten, is het gebruik van Application Control met Dynamic Whitelisting. Wanneer op een VM alleen vertrouwde software mag worden uitgevoerd, heeft malware geen schijn van kans. Met Kaspersky Security for Virtualization | Light Agent kunnen endpoint controls, waaronder Application Control, worden ingeschakeld op afzonderlijke VM's.

Bodiless malware

Een bepaalde vorm van geavanceerde malware heeft geen 'body', wat wil zeggen dat er niets kan worden gevonden in het bestandssysteem. Deze malware is afkomstig is van een eerder gestart uitvoerbaar bestand of is bij een inbraak binnengebracht, en kan zelden door traditionele anti-malwareoplossingen worden opgespoord. In een dergelijk geval zijn er geavanceerde anti-malwaretechnieken nodig die processen in het geheugen kunnen controleren en programma's die betrokken zijn bij verdachte of gevaarlijke activiteiten, onmiddellijk kunnen blokkeren.

Kaspersky Security for Virtualization | Light Agent is voorzien van diverse technologieën die voorkomen dat er in het geheugen van de VM wordt binnengedrongen. Deze omvatten:

- System Watcher, waarmee het gedrag van programma's wordt gecontroleerd en systeemgebeurtenissen worden gevolgd.
- Behavioral Stream Signatures, waarmee gedragspatronen worden geïdentificeerd die kenmerkend zijn voor malwareactiviteiten.

- Privilege Control, waarmee wordt voorkomen dat applicaties ongevraagde wijzigingen aanbrengen, waaronder procesinjectie.

Met deze tools kan het Host-based Intrusion Protection System (HIPS) schadelijke processen in het VM-geheugen opsporen en beëindigen.

Exploits

Het misbruik maken van vulnerability's in systeemonderdelen en populaire applicaties blijft een uiterst effectieve aanvalsmethode. Hoewel het mogelijk is met de eerder beschreven technologieën tegen te gaan dat er wordt binnengedrongen, kan het betreffende programma op een niveau met zulke hoge machtigingen werken dat de controle over de activiteiten van het programma wordt beperkt.

De meest effectieve methode om deze vorm van dreiging te bestrijden, is te voorkomen dat exploits misbruik kunnen maken van de beoogde vulnerability's. Om snel iets te doen aan de gevaren van niet-gepatchte vulnerability's, is Kaspersky Security for Virtualization | Light Agent voorzien van een technologie met de naam Automatic Exploit Prevention (AEP). AEP controleert met name de applicaties in belangrijke omgevingen zoals VDI die het vaakst het doelwit zijn, waaronder Adobe Reader, Internet Explorer, Microsoft Office, Java en vele andere, en biedt een extra niveau aan beveiligingscontrole en bescherming tegen onbekende dreigingen.

De efficiëntie van deze technologie heeft zich bewezen in onafhankelijke tests van het MRG Effitas-instituut, waarbij bleek dat zelfs bij uitschakeling van alle andere beveiligingsonderdelen Kaspersky's AEP-technologie 100% effectief bleef tegen aanvallen met behulp van exploits (zie Real World Enterprise Security Exploit Prevention, MRG Effitas, maart 2015 voor meer informatie). Zelfs onbekende zero-day-aanvallen worden door deze superieure technologie geblokkeerd.

Rootkits

Geavanceerde malware kan vaak zichzelf verbergen. Doordat dergelijke malware zogenaamde "bootkits" en "rootkits" gebruikt, is detectie door traditionele anti-malwareproducten niet mogelijk. Deze verraderlijke tools proberen de malware in een zo vroeg mogelijk stadium op te starten of uit te voeren, zodat er hoge machtigingen binnen het gastbesturingssysteem worden verkregen, wat helpt om onopgemerkt te blijven.

Zowel op het niveau van het geheugen als op het niveau van het bestandssysteem gebruikt Kaspersky Security for Virtualization | Light Agent de anti-rootkittechnologie van Kaspersky Lab om ook deze diep verborgen malware op te sporen en te elimineren.

Netwerkaanvallen

Aanvallers kunnen met cyberdreigingen via netwerken cruciale informatie over het netwerk verkrijgen, zich toegang verschaffen tot bepaalde bronnen van het systeem, kritische processen beïnvloeden en de werking van deze processen verstoren. Deze dreigingen omvatten kwaadaardige acties zoals het scannen van poorten, DoS-aanvallen (Denial of Service) en buffer-under-run-aanvallen. Zowel onze 'agentless' als 'light agent' oplossingen beschikken over ingebouwde netwerkbeveiligingstechnologieën. Bij Kaspersky Security for Virtualization | Light Agent worden de netwerkbeveiligingsmogelijkheden uitgebreid met ingebouwde HIPS (Host-based Intrusion Prevention System) en extra eigen technologieën voor het bestrijden van externe en interne netwerkaanvallen, waaronder dreigingen die mogelijk verborgen zijn in ondoorzichtig gevirtualiseerd verkeer.

Kaspersky Security for Virtualization | Agentless lost dit probleem ook op door gebruik te maken van de VMware-integratie om zo een Network Attack Blocker te bieden. Dit is een speciale virtuele applicatie die is ontworpen om netwerkverkeer te controleren op tekenen van typische aanvalsactiviteiten.

Schadelijke websites

Een van de meestvoorkomende besmettingsbronnen is een schadelijke of besmette website. Hoewel dit zelden gevolgen heeft voor gevirtualiseerde servers, kan dit een ernstige dreiging vormen voor VDI. Dit wordt niet altijd voldoende onderkend door zakelijke gebruikers. Op dit punt gaan de webbeveiligingstechnologieën van Kaspersky Lab een rol spelen.

Anti-phishing voorkomt dat gebruikers websites bezoeken die als gevaarlijk worden aangemerkt. Hierbij wordt gebruikgemaakt van informatie die is verkregen via het Kaspersky Security Network (KSN). Deze informatie wordt continu bijgewerkt met de hulp van miljoenen vrijwillige KSN-deelnemers overal ter wereld. Ook worden er nog niet ontdekte phishing-sites geblokkeerd dankzij een heuristische engine die de brontekst van de geladen pagina analyseert en tekenen van schadelijke code opspoort. Met de tools voor webbeheer kunt u het internetgebruik beheren. U kunt bijvoorbeeld de toegang blokkeren tot sociale netwerken, muziek, video, webmail die niet door het bedrijf is geïmplementeerd, evenals websites die ongepaste content bevatten of die niet voldoen niet aan bedrijfsbeleid. U kunt voor verschillende verantwoordelijkheden afwijkende beleidsregels implementeren en u kunt kiezen tussen een algehele blokkade of een beperkte blokkade tijdens bepaalde perioden.

Aanvallen op randapparatuur

De besmetting van een IT-netwerk via externe opslag is al lang een van de meest effectieve besmettingsmethoden. Weliswaar vormen besmettingen via het netwerk nu het grootste probleem vanwege de grote aantallen, maar externe storage blijft toch een aanzienlijk risico vormen, vooral wanneer deze onderdeel is van een zorgvuldig geplande, doelgerichte aanval. Verder dient u zich ervan bewust te zijn dat niet-beheerde apparatuur die niet voor storage bestemd is, ook een dreiging kan vormen. Externe storage-stations zijn één van de populairste methoden om vertrouwelijke gegevens te stelen. Hoewel het voor een niet-geautoriseerde persoon misschien niet gemakkelijk is toegang te krijgen tot de fysieke machines waarop uw virtuele infrastructuur wordt gehost, is het wel degelijk mogelijk.

Dus moet u altijd alert zijn bij hardware die op uw gevirtualiseerde omgeving wordt aangesloten. Zo worden er bij VDI-implementaties vaak thin-clients gebruikt en zelfs de eenvoudigste thin-clients hebben USB-poorten. Het beheer van randapparatuur kan een nachtmerrie zijn, of het kan probleemloos worden gedaan met behulp van Kaspersky Lab's Device Control-technologie. Met deze technologie kunt u opgeven welke verwisselbare apparaten toegang hebben tot afzonderlijke VM's, zodat u gemakkelijk een beheerbeleid kunt toepassen voor meerdere apparaten, waaronder verwisselbare stations, printers en verbindingen met andere netwerken dan het bedrijfsnetwerk.

Gegevenslekken

Het uitlekken van geheimen uit de IT-omgeving van een bedrijf is mogelijk niet alleen schadelijk voor bedrijfskritische processen of systemen, maar voor het hele bedrijf, inclusief reputatieschade die langdurige en pijnlijke gevolgen kan hebben. Beperking van het aantal manieren waarop informatie wordt gedeeld, is een goede optie om uw bedrijf te beveiligen.

Hiervoor kunt u gebruikmaken van zowel Kaspersky Lab's Application Control als Device Control. Met Application Control kan worden voorkomen dat gevaarlijke applicaties, zoals Instant Messaging-programma's of bestandshosting- en P2P-clientapps, worden uitgevoerd op de beveiligde VM. Met Device Control wordt het gebruik van externe storage beperkt, zodat de kans op diefstal van vertrouwelijke gegevens kleiner wordt. Kaspersky Security for Virtualization | Light Agent beschikt over beide technieken.

Agentless of light agent: welke optie is beter?

Het antwoord hangt af van welke virtualisatieplatform(s) u gebruikt, en van de specifieke implementaties. Ongeacht de hypervisor die wordt gebruikt voor het bouwen van uw gevirtualiseerde omgeving (VMware vSphere, Citrix XenServer, Microsoft Hyper-V of KVM) kunt u uw belangrijke virtuele servers en snel groeiende VDI beveiligen met Kaspersky Security for Virtualization | Light Agent. Maar u kunt ook overwegen Kaspersky Security for Virtualization | Agentless te gebruiken voor niet-kritieke VMware-servers waarvoor geen sterke meerlaagse beveiliging nodig is.

Gelukkig kunt u met het Kaspersky Security for Virtualization-licentiebeleid met één licentie de meest geschikte aanpak voor elk onderdeel van uw gevirtualiseerde omgeving implementeren: agentless, light agent of een combinatie van beide.

Bij alle combinaties van Citrix XenServer-, VMware vSphere-, KVM- of Microsoft Hyper-V-virtualisatieplatforms en bij alle methoden kunt u al uw virtuele en fysieke machines evenals de mobiele beveiliging eenvoudig en centraal beheren via één enkele gezamenlijke interface: Kaspersky Security Center. En onze cloudgebaseerde beveiligingsservice, Kaspersky Security Network, zorgt voor een bijna directe detectie van geavanceerde dreigingen.