TÁMOGATOTT PLATFORMOK:

- Microsoft Hyper-V Server 2008 R2 / 2012
- Citrix XenServer 6.0.2 / 6.1
- VMware ESXi 4.1, 5.0, 5.1 and 5.5

TÁMOGATOTT VENDÉG OPERÁCIÓS RENDSZEREK:

Telepítés módszere	Light Agent			Ügynökmentes
Virtuális gépre telepített vendég operációs rendszer	Windows Server 2008 R2 Hyper-V és Windows Server 2012 Hyper-V	Citrix Xen-Server 6.0.2 és 6.1	VMware ESXi 5.1 és 5.5	VMware ESXi 4.1, ESXi 5.0 vagy ESXi 5.1
Windows XP Professional SP3 (32-bites)	Igen	Igen	Nem	Igen
Windows XP Professional SP2 (64-bites)	Igen	Nem	Nem	Nem
Windows 7 Professional / Enterprise / Ultimate SP1 vagy újabb (32 / 64-bites)	Igen	Igen	Igen	Igen
Windows 8 Pro / Enterprise (32 / 64-bites)	Igen	Igen	Igen	Nem
Windows Vista Business / Enterprise / Ultimate SP2 (32-bit)es	Igen	Nem	Nem	Igen
Windows Server 2008 R2 Standard / Enterprise SP1 (64-bites)	Igen	Igen	Igen	Igen
Windows Server 2008 Standard / Enterprise SP2 (32 / 64-bites)	Igen	Igen	Igen	Igen
Windows Server 2003 R2 Standard / Enterprise SP2 (32 / 64-bites)	Igen	Nem	Igen	Igen
Windows Server 2003 Standard SP2 (32 / 64-bites)	Igen	Igen	Nem	Igen
Windows Server 2012 (64-bites)	Igen	Igen	Igen	Nem
Windows Small Business Server 2008 Standard (64-bites)	Igen	Nem	Nem	Nem
Windows Small Business Server 2011 Essentials / Standard (64-bites)	Igen	Nem	Nem	Nem

A Kaspersky Security for Virtualization megoldásra vonatkozó további információkért keresse helyi Kaspersky partnerét vagy látogasson el a **www.kaspersky.com** honlapra.

KSV/Version 3.1/April 14/Global

▶ KASPERSKY SECURITY FOR VIRTUALIZATION

Kiemelkedő, rugalmas és hatékony védelem virtuális szerver és desktop környezetek számára

FŐBB ELŐNYÖK

KIEMELKEDŐ VÉDELEM

- Támogatja a VMware, Microsoft Hyper-V és Citrix platformokat.
- Díjnyertes technológiánk a legösszetettebb rosszindulatú programok ellen is megvédi a virtuális számítógépeket (VM).
- A felhő alapú Kaspersky Security Network (KSN) integráció proaktív védelmet nyújt a felmerülő globális fenyegetések ellen.
- A rosszindulatú programok elleni fejlett védelem, például a biztonsági rés kiaknázások automata megelőzése (Automatic Exploit Prevention), erőteljes, többrétegű biztonságot nyújt.
- A (dinamikus fehérlistázást is magukba foglaló) alkalmazás vezérlők, illetve a web- és eszközvezérlők lehetővé teszik a rendszergazdáknak a szabályzatok érvényesítését, így a felhasználók biztonságban, produktívan dolgozhatnak.
- A VM-eket hálózati támadás blokkoló, tűzfal, hosztgép alapú behatolás megelőzés (HIPS) és adathalászat ellenes technológiák erőteljes kombinációja védi a hálózati fenyegetésektől.
- Az ügynökmentes VM-eket és az összes nem perzisztens VM-et azonnal és automatikusan védi a folyamatosan frissített biztonsági virtuális készülék (SVA).*

JOBB TELJESÍTMÉNY

- Az innovatív kialakítás alacsonyabb erőforrás-igényt támaszt, így optimalizálja a konszolidációs arányokat a maximális sűrűség érdekében.
- Az osztott gyorsítótár technológia megszünteti az ellenőrzésre fordított erőfeszítések duplikálását.
- Megszűnnek a vírusirtó frissítés és ellenőrzés miatti 'rohamok', illetve az azonnali bekapcsoláskor jelentkező biztonsági rések.

FOKOZOTT HATÉKONYSÁG

- Gyors, magától értetődő telepítés, amely nem igényel újraindítást, vagy a karbantartás üzemmódba lépést.
- Egyetlen konzolról együtt kezelhetők a fizikai, mobil és virtuális végpontok.
- Az egyszerűsített adminisztráció és bevezetés fokozott hatékonyságot, egyúttal kevesebb konfigurációs hibalehetőséget biztosít.
- Rugalmas licenckezelési lehetőségek — választható a (desktop vagy szerver-) gépek vagy erőforrások (magok) száma szerinti licenckezelés.

*A light agenttel működő perzisztens VM-ek a light agent telepítése után azonnal védelmet

A KASPERSKY SECURITY FOR VIRTUALIZATION OLYAN RUGALMAS MEGOLDÁS, AMELY VÉDELMET ÉS TELJESÍTMÉNYT EGYARÁNT BIZTOSÍT KÖRNYEZETE SZÁMÁRA.

A LEGFONTOSABB TERMÉKJELLEMZŐK

- Központi rendszerfelügyelet a Kaspersky Security Centerrel
- Központi VM védelem egyetlen SVA-val
- Rosszindulatú programok elleni fejlett védelem
- Hosztgép alapú behatolás megelőző rendszer (HIPS) tűzfallal
- Végponti alkalmazás-, hálózati hozzáférés és periféria felügyelet
- Felhő-támogatású biztonság a Kaspersky biztonsági hálózat (KSN) révén
- Hálózati támadások blokkolása
- Adathalászat elleni védelem
- Vírusvédelem IM, email és internetes forgalomhoz
- Új VM-ek esetén további telepítés vagy újraindítás nem szükséges*

BIZTONSÁGI VIRTUÁLIS KÉSZÜLÉK (SVA)

Ezen a területen a Kaspersky Lab két meggyőző megoldást nyújt, mindkettő egy biztonsági virtuális készüléken (SVA – Security Virtual Appliance) alapul.

A Kaspersky Lab SVA központosítva szkenneli a hosztkörnyezetben lévő összes VM-et. Ez az architektúra a végponti erőforrások feláldozása nélkül jelent hatékony védelmet a VM-eknek, ami nagyobb konszolidációs arányokat eredményez. Megszűnnek a vírusirtó ellenőrzés és frissítés miatti rohamok és az azonnali bekapcsoláskor jelentkező biztonsági rések.

A Kaspersky Security for Virtualization a VMware, Microsoft Hyper-V és CitrixXen platformokat, illetve ezek core technológiáit támogatja.

RUGALMAS LICENCKEZELÉS

Az önök igényeitől függően a Kaspersky Security for Virtualization megoldás a következő licenc-lehetőségekkel érhető el:

- Számítógép alapú licenckezelés:
  - Asztali számítógépenként
  - Szerverenként
- Erőforrás-alapú licenckezelés:
  - Magonként

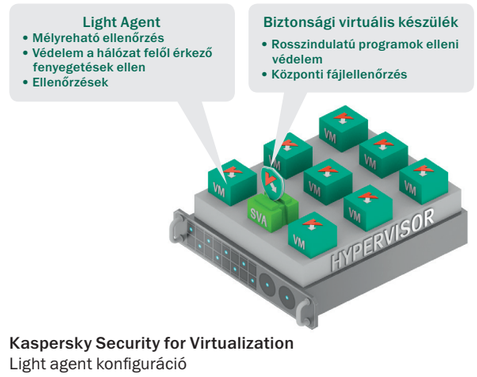
TÖBBFÉLE PLATFORM: EGYETLEN KÖLTSÉG

Egyetlen Kaspersky Security for Virtualization licenc magában foglalja a Citrix, Microsoft és VMware alapú virtuális környezetek támogatását.

* Nem perzisztens VM-ek esetén a light agent alkalmazás VM image-re történő telepítését követően azonnal rendelkezésre áll a védelem. Perzisztens VM-ek esetén a rendszergazdának a telepítés során manuálisan kell üzembe helyeznie a light agent-et.

LIGHT AGENT ALKALMAZÁS A FEJLETT VÉDELEM ÉRDEKÉBEN

A Kaspersky Security for Virtualization erőteljes, mégis alacsony erőforrás igényű ügynök alkalmazást tartalmaz, amely felkerül az összes virtuális gépre. Ez teszi lehetővé a fejlett végponti biztonsági funkciók aktiválását. Ilyenek például a sérülékenység megfigyelése, az alkalmazás, eszköz és web ellenőrzések, az azonnali üzenetküldő, email és böngészőprogramok vírusvédelme, illetve a fejlett heurisztika. Az eredmény: hatékony teljesítménnyel ötvözött erőteljes, többrétegű biztonság.

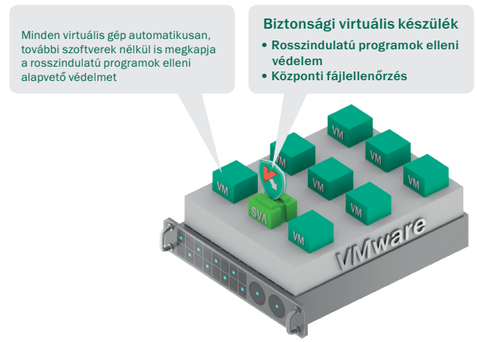


Kaspersky Security for Virtualization
Light agent konfiguráció

ÜGYNÖKMENTES KONFIGURÁCIÓ — VMWARE KÖRNYEZETEK

A VMware technológiákkal való szoros integráció azt jelenti, hogy a Kaspersky Security for Virtualization megoldás ügynökmentes biztonsági konfigurációban nagyon egyszerűen vezethető be és kezelhető ilyen platformokon. Minden biztonsággal kapcsolatos tevékenység a biztonsági virtuális készülékben koncentrálódik, amely a vShield megoldással áll összeköttetésben a virtuális gép azonnali és önműködő, illetve a vCloud alkalmazással a hálózat védelme érdekében.

Ebben a konfigurációban néhány fejlett biztonsági funkció, pl. fájl karantén, HIPS, fenyegetettség ellenőrzés és végpont ellenőrzések nem elérhetők.



Kaspersky Security for Virtualization
Ügynökmentes konfiguráció

Hagyományos ügynök-alapú	Ügynökmentes biztonság	Light Agent biztonság
• Bármelyik hypervisoron működik • Amikor a VM sűrűség nem kiemelt szempont • Windows, Linux vagy Mac vendég VM-ek	• Csak VMware alatt • Nagy VM sűrűséget tesz lehetővé • Csak Windows vendég VM-ek • Minimális informatikai erőforrás-igény a telepítéshez és felügyelethez • Tipikus telepítés: szerver virtualizáció ellenőrzött internetkapcsolattal (böngészés nincs)	• VMware, Citrix vagy Hyper-V • Nagy VM sűrűséget tesz lehetővé • Windows vendég VM-ek • Biztonsági és egyéb szabályzatok fejlett érvényesítése • Tipikus használat: kiemelt szerepkörű VDI és szerverek