LIGHT AGENT NEBO AGENTLESS

Průvodce ke Kaspersky Security for Virtualization

Stále oblíbenější virtualizace desktopů s sebou přináší i nové požadavky na vhodné zabezpečení. Přestože jsou virtualizované systémy na kyberútoky stejně citlivé jako běžný počítačový systém, vyznačují se některými zvláštnostmi, se kterými je třeba počítat při výběru bezpečnostního řešení.

Standardní bezpečnostní řešení, které nebylo vytvořeno s ohledem na požadavky virtuálního systému, může způsobovat několik vážných problémů:

1) **Enormní nároky na výkon.** Díky replikaci databází signatur a aktivních anti-malware filtrů na každém z chráněných virtuálních strojů (VM).
2) **„Lavina“.** Simultánní updaty databází a antimalware skeny běžící na více VM působí lavinový nárůst spotřeby zdrojů, vedoucí k výraznému poklesu výkonu a dokonce k nedostupnosti služeb. Pokusy o zmírnění tohoto problému navíc vytváří prostor pro útočníky. Odkládání malwarových skenů činí virtuálních stroje zranitelnějšími vůči útokům.
3) **Mezery při spuštění.** Na neaktivních VM se nemohou aktualizovat databáze signatur. V době mezi startem a ukončením aktualizace jsou tyto VM v ohrožení.
4) **Nekompatibilita.** Standardní systémy nejsou navrženy s ohledem na specifické potřeby virtualizovaného prostředí, jako jsou například migrace VM nebo absence fyzického hard disku a to může způsobit nestabilitu nebo dokonce zhroucení systému.

Důležitost zabezpečení virtuálních systémů a zachování unikátních možností, které virtualizace nabízí, vedla společnost VMware k vytvoření speciální obranné vrstvy vShield, určené pro platformu vSphere. Tato vrstva vytváří integrovaný bezpečný prostor obalující celý virtualizovaný systém a umožňuje jednoduchý a efektivní přístup virtualizovanému bezpečnostnímu řešení. Jednou z hlavních výhod je možnost vzniku „agentless“ ochrany virtualizovaných koncových stanic. Veškeré databáze signatur a engine pro antimalware skeny jedou na jediném speciálním virtuálním stroji - Security Virtual Appliace (SVA), což odebírá tuto zátěž jednotlivým samostatným VM a výrazně snižuje nároky na jejich výkon. Bezpečnostní řešení, schopná využívat vShield a virtualizované prostředí VMware, přinášejí svým uživatelům řadu výhod.

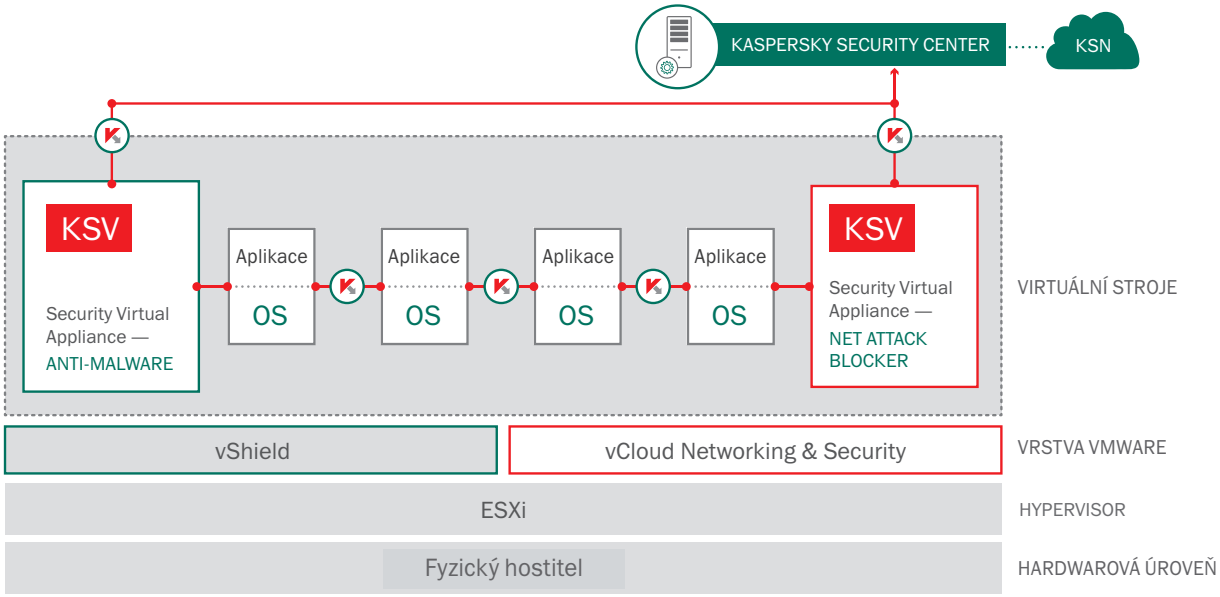
KASPERSKY SECURITY FOR VIRTUALIZATION | AGENTLESS

Kaspersky Security for Virtualization | Agentless byl vytvořen speciálně pro využití všech přínosů platformy vShield. Security Virtual Appliance (SVA) poháněná ceněným anti-malware enginem společnosti Kaspersky Lab je připravena k přímému nasazení - doslova “out-of-box”. Díky podpoře cloudové služby Kaspersky Security Network, reaguje systém v nejrychlejším možném čase a s minimálním počtem falešných poplachů (false positive). Technologii Kaspersky Network Attack Blocker může využívat ve spojení s komponentou vCloud Networking & Security spoločnosti VMware navíc i další SVA.

„Agentless“ přístup má ovšem i některé nedostatky.

Nevýhodou je, že společnost VMware je jediným výrobcem poskytujícím tento typ střední vrstvy zabezpečení, u ostatních platforem je tak nutné pro bezpečnostní řešení najít jiný způsob přístupu k jednotlivým VM.

Další komplikací je i to, že vrstva vShield neumožňuje přístup do vnitřních procesů jednotlivých VM, čímž je výrazně snížena schopnost bezpečnostních systémů ochránit síť VM před pokročilým malware ohrožením.

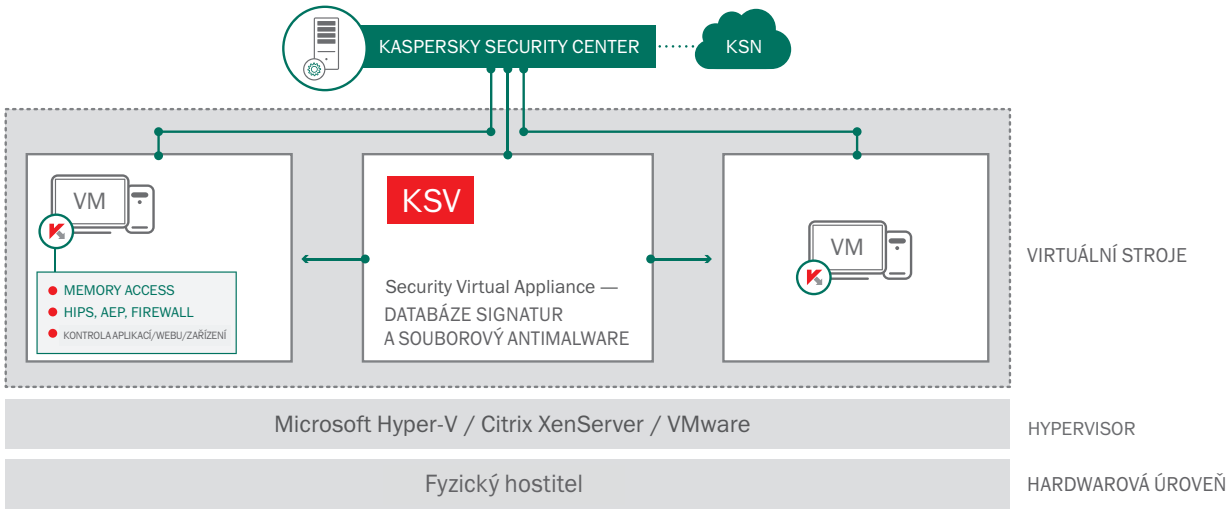


Firma Kaspersky Lab tato omezení překonala zavedením malé a „lehké“ aplikace na ochranu VM jako doplněk pro SVA. Tato aplikace, známá jako „light agent“, obsahuje jak skenovací engine, tak databáze, ale má, oproti plnohodnotné bezpečností aplikaci, mnohem menší požadavky na VM. Navíc poskytuje přístup nejenom k souborům uvnitř VM, ale i k jejich paměti a interním procesům. Důsledkem toho lze implementovat pokročilejší bezpečnostní techniky.

KASPERSKY SECURITY FOR VIRTUALIZATION | LIGHT AGENT

Kaspersky Security for Virtualization | Light Agent je aplikace vytvořená pro tři nejrozšířenější virtualizační platformy: VMware, Microsoft Hyper-V, Citrix. Anti-malware skener a databáze signatur jsou, stejně jako u agentless technologie, umístněné na přidělené SVA, čímž se uvolní zdroje VM pro zvýšení konsolidačních poměrů. S light agent aplikací uvnitř každého hostitelského OS, je možné implementovat ty nejpokročilejší bezpečnostní technologie, které jsou dostupné pro fyzické stroje, a to prostřednictvím **Kaspersky Endpoint Security for Business.** K dispozici je celá sada nástrojů pro ochranu koncových bodů, HIPS (Host-Based Intrusion Prevention System), vlastní firewall i nástroje pro správu systému. Je možné tak vytvořit mnohavrstvý obranný perimetr, odolný vůči sofistikovaným malware útokům a dokonce i zero-day ohrožení.

I přes vyšší úroveň ochrany, může někomu použití **Light agenta** připadat náročnější než nabízí jeho **agentless** řešení. **Light agent** sice vyžaduje více pozornosti při aplikaci do nových VM, ale tato omezení nejsou nijak zásadní. Abychom lépe pochopili rozdíly a výhody obou řešení, musíme se podívat hlouběji do jejich funkcionality i na rizika, před kterými jsou schopné systém chránit.



RIZIKA VS. MOŽNOSTI

Virtuální stroje jsou stejně nebo i více zranitelné jako jejich fyzické protějšky. Ve virtualizovaných sítích může mít rozšíření infekce skutečně devastující následky. Proto je důležité včas identifikovat bezpečnostní slabiny ve virtuální infrastruktuře, a implementovat nejvhodnější řešení. Podívejme se, jaká rizika ohrožují naše virtuální systémy a technologie a jak se jim účinně bránit.

SPUSTITELNÝ MALWARE

Ať už se do našeho systému dostane spustitelný malware formou přílohy k e-mailu nebo jako zábavná aplikace stažená z webu, ideálním protivníkem pro tento typ hrozby je anti-malware. Engine pro boj s malwarem je jádrem obou technologií řešení **Kaspersky Security for Virtualization** - jak **Agentless** tak **Light Agent** konfigurace. Rozdíl je pouze ve způsobu, jakým se dostává do souborových systémů chráněných VM.

Další formou jak chránit virtuální systém je nástroj Application Control s nasazením dynamického whitelistingu. Malware nemá šanci, pokud na počítači běží výhradně prověřené a bezpečné programy. Toho je možné dosáhnout pomocí řešení **Kaspersky Security for Virtualization | Light Agent**, které umožňuje spuštění kontroly aplikací na VM. Druhé řešení, **Kaspersky Security for Virtualization | Agentless,** operující prostřednictvím vShieldu, tuto možnost nenabízí.

MALWARE BEZE STOP

Některé sofistikované druhy malwaru nemají žádné „tělo“, dohledatelné v souborovém systému. Bez ohledu na to, zda se do systému dostane prostřednictvím dříve spuštěného škůdce nebo si najde nějaké zranitelné místo v systému, tento malware není možné najít pomocí běžného anti-malware softwaru. Na takový kalibr je nutné nasadit Anti-malware systémy schopné dohlížet na jednotlivé procesy v paměti a okamžitě blokovat programy, účastnící se podezřelých nebo nebezpečných aktivit.

+**Kaspersky Security for Virtualization | Light Agent** je vybaven řadou technologií schopných blokovat útoky na VM.

- **System Watcher** – monitoruje chování programů a systémových událostí.
- **Technologie BSS** – Behavioral Stream Signatures, podporuje System Watcher a identifikuje behaviorální schémata typická pro aktivity malwaru.
- **Správa práv** – omezuje aplikace v provádění změn, včetně injektáže procesů.

Tyto nástroje umožňují systému Host-Based Intrusion Prevention System (HIPS) najít a zastavit nebezpečné procesy v paměti VM.

Kaspersky Security for Virtualization | Agentless je vzhledem k API omezením v prostředí vShieldu, schopen sledovat pouze změny na úrovni souborového systému.

EXPLOITY

Využívání zranitelnosti systému a populárních aplikací patří mezi nejefektivnější cesty k napadení systému. Přestože je možné útoku čelit pomocí výše zmiňovaných technologií, napadený program s vysokým oprávněním a omezenou kontrolou jeho aktivit, může způsobit problémy.

Nejúčinnější metodou boje proti tomuto typu ohrožení je ochrana vůči exploitům, jejíchž prvotním cílem je využívání zranitelných míst. Toho je možné docílit rozpoznáním sekvencí aktivit typických pro exploity a jejich zastavením. K tomu je určen systém Kaspersky Automatic Exploit Prevention (AEP). Efektivita této technologie byla prověřena řadou testů nezávislého institutu MFG Effitas. Během těchto testů bylo prokázáno, že i po vypnutí všech ostatních obranných součástí, zůstává AEP technologie Kaspersky 100% účinná proti útokům využívajícím exploity a dokáže zablokovat i dosud neznámé zero-day exploity.

AEP je součástí řešení **Kaspersky Security for Virtualization | Light Agent**, což z něj činí vynikající nástroj pro virtuální desktopové systémy (VDI) s vyšším rizikem ohrožení, spojeným s používáním externích disků.

Kaspersky Security for Virtualization | Agentless touto funkcí nedisponuje a musí se spoléhat na schopnosti vShieldu.

ROOTKITY

Sofistikovaný malware je schopen se pomocí „bootkitů“ a „rootkitů“ ukrývat a bránit se odhalení běžným anti-malwarem. Tito nebezpeční útočníci se snaží spustit malware co nejdříve, aby nemohl být odhalen a získal co možná nejvyšší systémová práva. Technologie Kaspersky Anti-Rootkit je schopna najít a odstranit i takto ukrytý malware. Operuje totiž jak v paměti, tak v souborovém systému, s přístupem do RAM a procesů konkrétního hostitelského stroje.

Technologie Kaspersky Anti-Rootkit je součástí řešení **Kaspersky Security for Virtualization | Light Agent**, díky kompletnímu přístupu do všech zdrojů hostitelského stroje.

Kaspersky Security for Virtualization | Agentless může vstoupit pouze do souborového systému, tudíž nedisponuje schopností odhalovat rootkity.

SÍŤOVÉ ÚTOKY

Existují hrozby, které využívají vlastností síťových systémů, umožňující získat útočníkovi důležité informace o síti před útokem, nebo zajistit přístup k vybraným systémovým zdrojům a narušit jejich bezproblémový chod. Patří mezi ně například skenování portů, DOS a DDOS útoky, přetečení zásobníků a podobně. K obraně před těmito útoky slouží speciální nástroje technologie Kaspersky Network Attack Blocker. Tato technologie dokáže pomocí IDS (Intrusion Detection System) zabránit síťovým útokům a s pomocí heuristických algoritmů rozezná i ta nejkomplexnější schémata útoku.

Systémy **Kaspersky Security for Virtualization | Light Agent a Kaspersky Security for Virtualization | Agentless** mají tuto síťovou technologii ve svém arzenálu.

ŠKODLIVÉ WEBOVÉ STRÁNKY

Jedním z nejběžnějších zdrojů infekce jsou škodlivé nebo infikované webové stránky. I když většinou přímo neohrožují virtualizovaný server, mohou představovat vážné nebezpečí pro VDI řešení s neomezeným přístupem k internetu. Webová technologie Anti-phishing společnosti Kaspersky Lab brání uživatelům vstoupit na stránky označené jako nebezpečné. Využívá totiž informací z Kaspersky Security Network - databáze nepřetržitě aktualizované miliony dobrovolných účastníků z celého světa. Pomocí heuristického enginu, který analyzuje zdrojový text stránky a hledá stopy škodlivého kódu, jsou blokovány i dosud neobjevené phishingové stránky. Technologie Web Control umožňuje také omezit přístup na nejrůznější herní stránky nebo sociální sítě. Brání tak uživatelům plýtvat v práci časem a věnovat se nepracovním aktivitám.

Tuto technologii nabízí pouze **Kaspersky Security for Virtualization | Light Agent.** Je tedy vhodnější pro ochranu VDI systémů s přístupem na internet.

ÚTOKY POMOCÍ PERIFERIÍ

Externí zařízení (např. disk) patří k nejefektivnějším metodám infikování IT sítě. I když jsou útoky po síti v poměru počtu výskytů četnější, externí disky představují stále výraznou hrozbu. A to především ve spojení s dobře naplánovaným a přesně mířeným útokem. Potenciálním nebezpečím mohou být i externí zařízení bez hard disku. Jsou doloženy případy s infikovaným firmwarem síťové tiskárny. Externí disk je však stále nejčastější cestou, kterou důvěrná data opouštějí vaši společnost.

Přestože není nijak jednoduché, aby se nepovolaná osoba dostala k hardwaru hostícímu vaši virtuální infrastrukturu, ta možnost tu stále je. V některých případech to představuje příliš velké riziko. Navíc při nahrazení koncových stanic VDI řešením, může mít i ten nejjednodušší klient USB port.

Kontrola a správa periferií je důležitým opatřením, které dokonale zajišťuje technologie Kaspersky Device Control. Ta umožňuje nastavit omezení specifických periferií a konfigurovat výjimky tak, aby nebyly ohroženy běžné pracovní činnosti.

Device Control nabízí pouze **Kaspersky Security for Virtualization | Light Agent**, řešení **Kaspersky Security for Virtualization | Agentless** jej neobsahuje.

ÚNIK DAT

Únik firemních dat a tajných informací z IT sítě může společnosti způsobit velké problémy, včetně poškození jména, které mívá dlouhodobé a bolestivé důsledky. Prospěšným řešením je omezení možností sdílení informací.

K tomu je možné využít technologie Application Control a Device Control. Application Control brání spuštění nebezpečných aplikací, jako je například instant messenger, sdílení souborů a P2P aplikacím. Device Control omezuje užívání externích úložných zařízení, která mohou sloužit pro vynášení citlivých dat.

Obě technologie jsou součástí K**aspersky Security for Virtualization | Light Agent,** ale nelze je využívat v **Kaspersky Security for Virtualization | Agentless.**

AGENTLESS VS LIGHT AGENT: KTERÝ JE LEPŠÍ?

Na první pohled je odpověď jasná: **Kaspersky Security for Virtualization | Light Agent** je vybavený pokrokovými technologiemi, které **Kaspersky Security for Virtualization | Agentless** nemá. Zdá se, že řešení s použitím „light agenta“ je jednoznačně lepší.

Ale nedělejme předčasné závěry, je to trochu složitější.

Zaprvé je tu okamžitá ochrana prostřednictvím **Kaspersky Security for Virtualization | Agentless.** Virtuální stroje jsou chráněny od okamžiku jejich startu, což může být důležité, pokud už se infekce ve vašem systému stala nezvladatelnou a vaše VM není možné nastartovat pomocí image disku s aplikací Light agent.

V některých případech získává **Kaspersky Security for Virtualization | Agentless** výhodu nad **Kaspersky Security for Virtualization | Light Agent** v oblasti výkonu.

Pro výběr nejlepšího zabezpečení pro váš virtuální systém je třeba zvážit potenciální hrozby, hodnotu dat, která mají být chráněna a různé úrovně potřebné ochrany. *

Poznámka na závěr.
Jakákoliv kombinace agentless ochrany pro VMware a ochrany s light agentem pro všechny tři platformy je pokryta jednotnou licencí **Kaspersky Security for Virtualization.** Nezáleží na tom, jestli využíváte platformu VMware, Microsoft nebo Citrix, všechno můžete řídit pohodlně z jednotné ovládací konzole **Kaspersky Security Center.**

* Pro více informací k volbě nejlepší kombinace bezpečnostních řešení společnosti Kaspersky Lab pro ochranu vaší virtuální infrastruktury, si přečtěte whitepaper „Kaspersky Security for Virtualization: Understand the Difference“

KASPERSKY lab