SOLUZIONE CON LIGHT AGENT O AGENTLESS

Guida alle funzioni di Kaspersky Security for Virtualization

Con la crescente diffusione della virtualizzazione, la necessità di utilizzare adeguate soluzioni di protezione è ovvia. Anche se altrettanto vulnerabili ai cyber attacchi di qualsiasi altro sistema fisico, gli ambienti virtuali presentano funzioni specifiche che vanno considerate al momento di scegliere la soluzione di sicurezza più appropriata.

Le soluzioni standard non specificamente progettate per gli ambienti virtuali, oltre a fornire un determinato livello di protezione, possono introdurre alcuni problemi, quali:

1) **Consumo eccessivo delle risorse** a causa della replica dei database delle firme e dei motori anti-malware attivi su ciascuna macchina virtuale (VM) protetta.
2) **"Storm"**: aggiornamenti simultanei dei database e/o processi di scansione anti-malware su più VM che conducono ad un aumento "effetto valanga" del consumo di risorse, causando un drastico peggioramento delle prestazioni e, persino, attacchi DoS (Denial of Service). I tentativi di risolvere il problema programmando questi processi generano le cosiddette "finestra di vulnerabilità", ossia periodi in cui il posticipo delle scansioni malware rende la VM vulnerabile agli attacchi.
3) **Falle di sicurezza**. Non è possibile aggiornare i database delle firme su VM inattive, pertanto dall'avvio della macchina al completamento del processo di aggiornamento, la VM diventa vulnerabile agli attacchi.
4) **Incompatibilità.** Poiché le soluzioni standard non sono concepite per gestire funzioni specifiche per la virtualizzazione, come la migrazione di VM o l'archiviazione non persistente, il loro utilizzo può causare instabilità e, persino, blocchi al sistema.

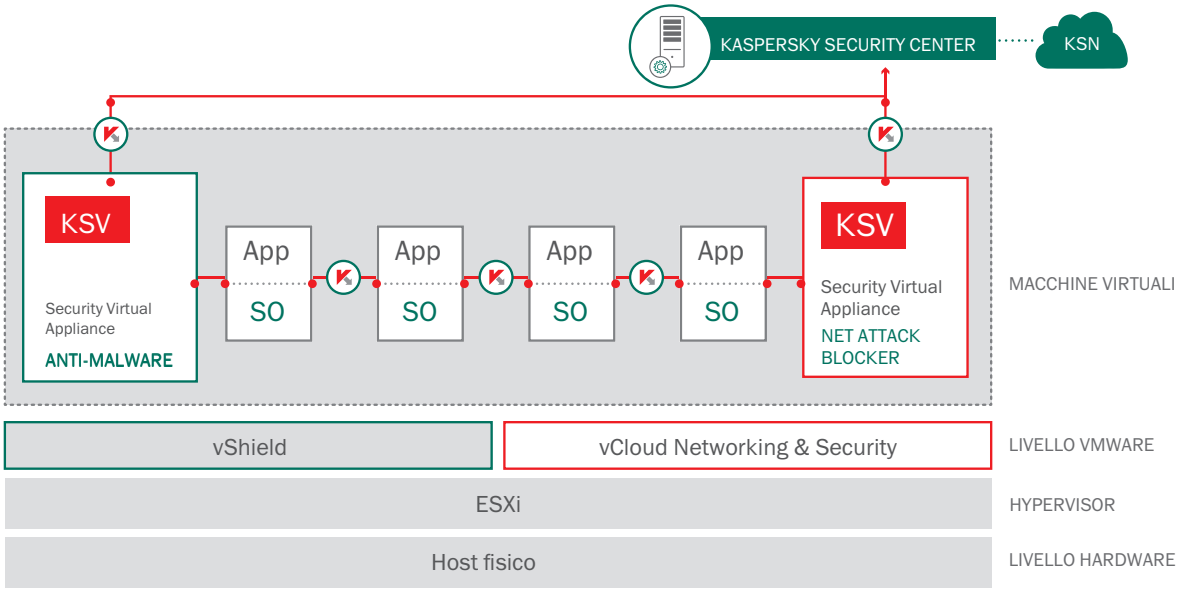
Riconoscendo l'importanza della sicurezza dei sistemi virtuali e le esclusive funzioni offerte dalla virtualizzazione, VMware, azienda leader del settore, ha sviluppato vShield, uno specifico livello di difesa per la sua piattaforma vSphere. Questo livello crea uno spazio di sicurezza integrato riunendo tutte le risorse virtualizzate e consentendo un accesso facile ed efficiente mediante le soluzioni di sicurezza appositamente progettate. Un ovvio vantaggio derivante da questo approccio consiste nella protezione "agentless" degli endpoint virtualizzati, che diventa un'opzione. Poiché è richiesta una sola Security Virtual Appliance (SVA), ossia una macchina virtuale specializzata che include un motore di scansione anti-malware e i database delle firme, le singole VM sono liberate da questo carico di lavoro e il consumo di risorse viene notevolmente ridotto. Le soluzioni di sicurezza compatibili con vShield, in grado di avvalersi di tutte le funzioni offerte dall'ambiente di VMware, possono assicurare agli utenti numerosi vantaggi tramite questo approccio.

KASPERSKY SECURITY FOR VIRTUALIZATION | AGENTLESS

La soluzione Kaspersky Security for Virtualization | Agentless è stata appositamente progettata per usufruire di tutti i vantaggi offerti da vShield. Una Security Virtual Appliance (o SVA), immediatamente pronta per una rapida implementazione, contiene il pluripremiato motore anti-malware di Kaspersky Lab, che le consente di usufruire dei vantaggi derivanti da tassi di rilevamento superiori. Il supporto del servizio assistito da cloud Kaspersky Security Network garantisce i tempi di reazione più rapidi e, soprattutto, riduce notevolmente il numero dei falsi positivi. È possibile utilizzare una seconda SVA per fornire la tecnologia Network Attack Blocker di Kaspersky insieme al componente VMware vCloud Networking & Security.

Tuttavia, un approccio "agentless" comporta anche alcuni svantaggi.

Innanzitutto, VMware è l'unico fornitore che offre un livello di protezione intermedio; per altre piattaforme, le soluzioni di sicurezza devono trovare un altro modo per accedere alle singole VM. In secondo luogo, vShield non fornisce l'accesso ai processi interni delle macchine virtuali, diminuendo notevolmente la capacità delle soluzioni di offrire una protezione ottimale dalle avanzate minacce malware a questo livello.



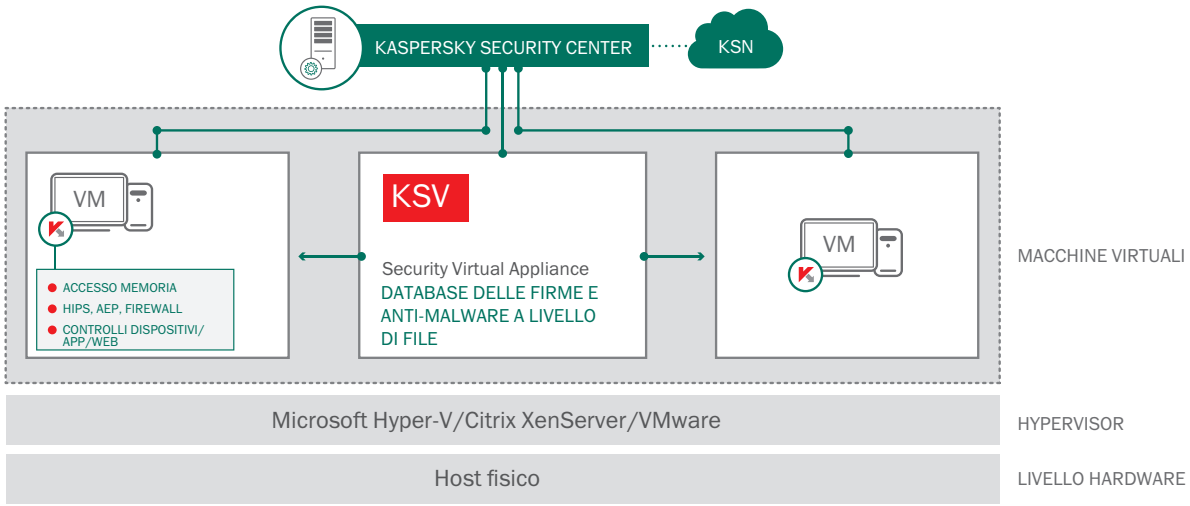
Per superare queste limitazioni, è stato introdotto un altro approccio, che prevede l'implementazione di una piccola applicazione alla VM da proteggere oltre alla SVA. Questa applicazione è nota come "light agent." Anche se il motore di scansione dei file e i database vengono comunque memorizzati a livello centrale, questa applicazione occupa una quantità di memoria della VM estremamente ridotta rispetto ad una soluzione basata su un agente completo, offrendo, al contempo, l'accesso non solo al file system della VM, ma anche alla sua memoria e ai relativi processi interni. Di conseguenza, è possibile impiegare altre tecniche di protezione più avanzate.

KASPERSKY SECURITY FOR VIRTUALIZATION | LIGHT AGENT

La soluzione Kaspersky Security for Virtualization | Light Agent è stata creata per le tre più importanti piattaforme di virtualizzazione: Citrix, Microsoft Hyper-V e VMware. Lo scanner anti-malware e i database delle firme risiedono in una SVA dedicata, come nel caso della tecnologia agentless, liberando le risorse grazie all'implementazione di VM aggiuntive per ottimizzare i tassi di consolidamento. Inoltre, grazie alla presenza di un "light agent" all'interno di ciascun sistema operativo guest, è possibile impiegare la maggior parte delle tecnologie avanzate disponibili nelle macchine fisiche tramite **Kaspersky Endpoint Security for Business**. È possibile implementare una gamma completa di controlli degli endpoint, nonché un sistema di prevenzione delle intrusioni basato su host (HIPS, Host-Based Intrusion Prevention System), un firewall proprietario e una serie di strumenti per la gestione dei sistemi. Ne consegue la creazione di un perimetro difensivo multilivello, in grado di far fronte ai più sofisticati esempi di malware e, persino, alle minacce "Zero Day".

Ovviamente, benché sia in grado di fornire un livello di protezione superiore, la soluzione basata su un **"light agent"** potrebbe apparire "più pesante" della sua controparte **agentless**, anche perché è richiesta una maggiore attenzione durante l'implementazione di nuove VM. Tuttavia, anche queste caratteristiche non sono così immediate da capire.

Per una migliore comprensione, dobbiamo analizzare più in dettaglio le funzionalità delle soluzioni **agentless** e quelle basate su un **"light agent"** e le minacce che sono in grado di contrastare.



MINACCE E FUNZIONALITÀ

Le macchine virtuali sono vulnerabili tanto quanto le loro controparti fisiche e, forse, anche di più: nelle reti virtualizzate ad alta velocità, la diffusione delle infezioni può avere risultati devastanti. È importante, pertanto, identificare le falle di sicurezza nell'infrastruttura virtuale e implementare misure adeguate alle potenziali minacce. Di seguito, verranno esaminate le potenziali minacce ai sistemi virtuali e le tecnologie utilizzate per contrastarle.

FILE MALWARE ESEGUIBILI

Sia che si tratti di un allegato dannoso ricevuto tramite email, di un gioco infetto o di un eseguibile temporaneo creato da un malware, una protezione anti-malware è fondamentale per fronteggiare queste minacce basilari. Il motore anti-malware rappresenta la tecnologia fondamentale delle configurazioni **agentless** e basate su un **"light agent "** della soluzione **Kaspersky Security for Virtualization**, sebbene i file system della VM protetta vengano raggiunti in modi diversi a seconda dei casi.

Un altro modo per impedire agli agenti malware di danneggiare le risorse virtualizzate consiste nell'utilizzo della funzionalità Application Control con whitelisting dinamico. Consentendo solo l'esecuzione di software attendibile e sicuro, il malware viene interrotto sul suo percorso. La soluzione Kaspersky Security for Virtualization | Light Agent consente di attivare la funzionalità Application Control sulle VM, al contrario la soluzione Kaspersky Security for Virtualization | Agentless, che funziona tramite vShield, non supporta i controlli degli endpoint.

MALWARE "SENZA CORPO"

Alcuni malware sofisticati si presentano "senza corpo", ossia non sono rilevabili nel file system. Generati da un eseguibile avviato in precedenza o infettati tramite un exploit, questi tipi di malware sfuggono al rilevamento effettuato mediante un programma anti-malware tradizionale. In questi casi, sono richieste soluzioni anti-malware più avanzate in grado di controllare i processi in memoria e bloccare immediatamente i programmi coinvolti in attività sospette o totalmente pericolose. La soluzione **Kaspersky Security for Virtualization | Light Agent** è dotata di una gamma di tecnologie in grado di bloccare eventuali attacchi alla memoria della VM, Queste includono:

- System Watcher, che controlla il comportamento dei programmi, tenendo traccia degli eventi di sistema. Questa funzionalità è supportata dai seguenti strumenti:
- BSS (Behavioral Stream Signatures), che consente di identificare gli schemi di comportamento caratteristici dell'attività di un malware.
- Privilege Control, che impedisce all'applicazione di apportare modifiche non richieste, come nel caso in cui un processo "inietta" il proprio codice dannoso.

Questi strumenti consentono al sistema di prevenzione delle intrusioni basato su host (HIPS, Host-based Intrusion Protection System) di tenere traccia e interrompere eventuali processi non autorizzati nella memoria della VM.

La soluzione Kaspersky Security for Virtualization | Agentless è in grado di tenere traccia delle modifiche apportate solo al livello del file system a causa delle limitazioni dell'API vShield.

EXPLOIT

Lo sfruttamento delle vulnerabilità presenti nei componenti dei sistemi e nelle applicazioni più comuni rimane tra i meccanismi di attacco più efficaci. Benché sia possibile vanificare l'efficacia di questi attacchi mediante le suddette tecnologie, è possibile scegliere di eseguire i programmi interessati con privilegi elevati in modo da limitare il controllo sulle relative attività.

Il metodo più efficace per affrontare queste minacce consiste nell'impedire agli exploit di effettuare il lavoro per cui sono progettati, ossia sfruttare innanzitutto le vulnerabilità presenti. Questo risultato viene conseguito riconoscendo la sequenza delle azioni caratteristiche degli exploit, ad esempio, tramite la funzionalità di prevenzione automatica degli exploit (AEP) di Kaspersky. L'efficienza di questa tecnologia è stata comprovata da una serie di test indipendenti condotti dall'istituto MRG Effitas. Questi test hanno dimostrato come, anche con tutti gli altri componenti di protezione disattivati, la tecnologia AEP di Kaspersky sia rimasta efficiente al 100% contro gli attacchi che utilizzano exploit. Anche se sconosciuti, gli exploit "zero-day" vengono bloccati da questa tecnologia proattiva.

La soluzione Kaspersky Security for Virtualization | Light Agent è dotata di questa funzione avanzata, che risulta particolarmente utile nelle VDI (Virtual Desktop Infrastructures) impiegate per sostituire i desktop fisici con i loro elevatissimi rischi di contrarre infezioni dovute a download indesiderati.

La soluzione Kaspersky Security for Virtualization | Agentless deve basarsi sulle funzionalità vShield, che mancano di alcune funzioni analogamente alla tecnologia AEP di Kaspersky.

ROOTKIT

Gli attacchi malware sofisticati sono spesso capaci di nascondersi, sfuggendo al rilevamento effettuato mediante un programma anti-malware tradizionale, grazie all'aiuto dei cosiddetti "bootkit" e "rootkit". Questi insidiosi strumenti tentano di caricare il malware appena possibile in modo da ritardarne la scoperta ottenendo privilegi elevati all'interno del sistema. La tecnologia anti-rootkit di Kaspersky è in grado di rilevare ed eliminare anche questo tipo di malware nascosto in profondità. Questa tecnologia opera nella memoria e al livello del file system, richiedendo l'accesso ai processi e alla RAM della macchina guest per funzionare.

La soluzione Kaspersky Security for Virtualization | Light Agent può offrire questa tecnologia perché dispone dell'accesso completo alle risorse della macchina guest.

La soluzione Kaspersky Security for Virtualization | Agentless può accedere, invece, solo al file system, pertanto non dispone della piena funzionalità anti-rootkit.

ATTACCHI DI RETE

Alcune minacce traggono vantaggio dalle funzioni del sistema di rete, consentendo all'autore dell'attacco di acquisire informazioni fondamentali sulla rete attaccata, ottenere l'accesso alle risorse del sistema oggetto dell'attacco o interferire con il corretto andamento delle operazioni. Tra queste minacce, figurano: scansione di porte, attacchi DoS (Denial-of-Service), attacchi che provocano errori di sottocarico del buffer e altri attacchi dannosi. Questi tipi di attacchi richiedono contromisure specifiche simili a quelle fornite dalla funzionalità Network Attack Blocker di Kaspersky. Come suggerisce il suo nome, questa tecnologia blocca gli attacchi in arrivo sulla rete con l'aiuto di un sistema IDS (Intrusion Detection System) mediante l'utilizzo di algoritmi euristici per distinguere persino i più complessi modelli di attacco.

Sia la soluzione **Kaspersky Security for Virtualization | Agentless** che **Kaspersky Security for Virtualization | Light Agent** dispongono di queste tecnologie di rete nei loro arsenali.

SITI WEB DANNOSI

Una delle fonti più comuni di infezione deriva da un sito Web dannoso o infetto. Anche se raramente interessa i server virtualizzati, un sito Web di questo tipo può costituire una seria minaccia per i desktop virtualizzati (VDI) se agli utenti viene consentito un accesso completo a Internet. A questo punto, entrano in gioco le tecnologie Web di Kaspersky. Una protezione anti-phishing impedisce agli utenti di accedere ai siti Web segnalati come pericolosi, utilizzando le informazioni ottenute tramite **Kaspersky Security Network** e costantemente aggiornate con l'aiuto di milioni di volontari KSN in tutto il mondo. Anche siti di phishing non ancora rilevati vengono bloccati grazie ad un motore euristico che analizza il testo sorgente della pagina caricata, rilevando eventuali tracce di codici dannosi. La tecnologia **Web Control** presenta l'ulteriore vantaggio di restringere l'accesso ai siti Web non correlati ad attività lavorative, come i siti di giochi o i social network, impedendo agli utenti di perdere tempo prezioso in operazioni inutili.

La soluzione Kaspersky Security for Virtualization | Agentless non possiede queste funzioni basate su host, al contrario della soluzione **Kaspersky Security for Virtualization | Light Agent**, che, pertanto, risulta più adatta ai VDI con accesso a Internet.

ATTACCHI BASATI SULLE PERIFERICHE

Tradizionalmente, uno dei metodi più efficaci per introdurre un'infezione in una rete IT consiste nell'utilizzare un dispositivo di archiviazione esterno. Anche se le infezioni che si trasmettono in rete ora sembrano la minaccia maggiore da un punto di vista numerico, i dispositivi di archiviazione esterni rimangono comunque notevolmente pericolosi, specialmente se fanno parte di un attacco mirato accuratamente pianificato. Vale la pena ricordare che anche le perifiche di archiviazione non controllate possono costituire una minaccia; tra i casi noti, ad esempio, figura il firmware infetto delle stampanti. Inoltre, le unità di archiviazione esterne rimangono tra i metodi principali per la memorizzazione di dati riservati durante gli spostamenti.

Benché non sia solitamente facile per un utente non autorizzato ottenere l'accesso alle macchine fisiche che ospitano l'infrastruttura virtuale, questa situazione può comunque verificarsi e, in alcuni casi, una tale eventualità è considerata come un rischio troppo elevato. Inoltre, per quanto riguarda i desktop virtualizzati (VDI), anche i più semplici thin-client possono disporre di porte USB.

Pertanto, il controllo delle periferiche diventa una precauzione ragionevole, che viene facilmente eseguita tramite la tecnologia **Device Control** di Kaspersky. In tal modo, è possibile prevenire o limitare l'utilizzo di tipi di bus e dispositivi specifici. Inoltre, ovviamente, è possibile configurare alcune eccezioni, in modo da consentire di utilizzare le periferiche essenziali per svolgere le attività lavorative.

Per quanto riguarda le altre tecnologie di controllo, la funzionalità Device Control viene offerta all'interno della soluzione **Kaspersky Security for Virtualization | Light Agent**, ma non nella soluzione **Kaspersky Security for Virtualization | Agentless**.

FUGA DI DATI

La fuga di segreti aziendali da una rete IT può infliggere un enorme danno ad un'azienda, che può incidere sulla sua reputazione con conseguenze dolorose e durature. Pertanto, può diventare necessario limitare le modalità di condivisione delle informazioni. A questo punto, risultano utili le soluzioni **Application Control** e **Device Control** di Kaspersky. La funzionalità Application Control può impedire l'esecuzione di applicazioni pericolose, come i servizi di messaggistica istantanea o l'hosting dei file e le applicazioni client P2P, mentre la funzionalità Device Control limita l'utilizzo dei dispositivi di archiviazione esterni, che possono essere utilizzati per memorizzare dati sensibili.

Come già detto in precedenza, queste due tecnologie vengono incluse all'interno della soluzione **Kaspersky Security for Virtualization | Light Agent**, ma non nella soluzione **Kaspersky Security for Virtualization | Agentless.**

SOLUZIONE AGENTLESS O CON "LIGHT AGENT": QUAL È LA MIGLIORE?

Per alcuni utenti, la risposta a questa domanda potrebbe sembrare semplicissima: la soluzione **Kaspersky Security for Virtualization | Light Agent** è dotata di funzioni avanzate, che non sono incluse nella soluzione **Kaspersky Security for Virtualization | Agentless**, pertanto la soluzione con "light agent " è ovviamente la migliore. In realtà, bisogna prestare attenzione a non arrivare frettolosamente alle conclusioni: la situazione è leggermente più complicata.

In primo luogo, occorre considerare la questione della protezione immediata offerta dalla soluzione **Kaspersky Security for Virtualization | Agentless**. Le macchine virtuali vengono protette immediatamente dopo il loro avvio, un'operazione che può risultare di fondamentale importanza se un'infezione è già in circolazione in una rete virtualizzata senza alcun controllo (mentre non è possibile avviare la VM da un'immagine contenente l'applicazione **Light Agent**).

Nuovamente, in alcuni casi, la soluzione **Kaspersky Security for Virtualization | Light Agent** può risultare inferiore alla soluzione **Kaspersky Security for Virtualization | Agentless** in termini di prestazioni. Per scegliere l'opzione di sicurezza migliore per la propria installazione virtuale e ottenere il massimo da ogni progetto di virtualizzazione, è necessario valutare attentamente le potenziali minacce, il valore dei dati da proteggere e i diversi livelli di protezione richiesti*.

Si prega di notare che qualsiasi combinazione di protezione agentless per VMware e sicurezza basata su un "light agent" per una o tutte e tre le piattaforme è coperta da una sola licenza di **Kaspersky Security for Virtualization**. Sia che venga utilizzata una piattaforma Citrix, VMware o Microsoft, la pratica interfaccia comune di **Kaspersky Security Center** consente di tenere tutto sotto controllo.

* Per ulteriori informazioni sulla scelta della migliore combinazione di soluzioni Kaspersky per la protezione dell'infrastruttura virtuale, leggere il whitepaper "Kaspersky Security for Virtualization: Understand the Difference" (Kaspersky Security for Virtualization: come capire la differenza).

KASPERSKY lab