KASPERSKY lab

SICUREZZA DEGLI AMBIENTI VIRTUALI: CAPIRE LA DIFFERENZA

www.kaspersky.it

SICUREZZA DEGLI AMBIENTI VIRTUALI: CAPIRE LA DIFFERENZA

Se state già attuando la conversione delle vostre risorse hardware in un ambiente virtuale, l'obiettivo aziendale è quasi certamente quello di ottenere la massima efficienza dall'infrastruttura IT. L'esecuzione congiunta di varie macchine virtuali (VM) su un unico computer anziché utilizzare server dedicati, ognuno dei quali necessita singolarmente di alimentazione, raffreddamento e gestione, è un argomento convincente. Più nodi virtualizzati basati su un singolo server fisico determinano un risparmio per l'azienda. L'effetto economico della virtualizzazione può essere estremamente potente: secondo un sondaggio condotto da Forrester nel 2011, l'implementazione di un'infrastruttura VMware VDI ha determinato un ROI ponderato in base al rischio del 255% in un periodo di 4 anni, con un punto di pareggio a 17 mesi dall'implementazione.

La domanda è: quante VM è possibile inserire in tale configurazione hardware senza produrre un notevole impatto sulle prestazioni? Questo è ciò che viene definito "tasso di consolidamento" e che costituisce la parte realmente complessa, con una molteplicità di fattori da considerare. Che tipo di attività si suppone che debba essere svolto dalle macchine virtuali? Quale software hypervisor si utilizza? Quali rischi si corrono collocando tutte le risorse in così pochi contenitori? E come proteggere in modo affidabile la nuova infrastruttura virtuale, assicurandosi di non essere vulnerabili ai cybercriminali, senza arrivare agli estremi e rallentare tutto a passo di lumaca? Per prendere la decisione giusta, è necessario comprendere alcuni concetti ed esaminare il modo in cui interagiscono.

MODELLI DI VIRTUALIZZAZIONE

Il settore ha definito vari modelli di virtualizzazione. In questo documento ne vengono considerati quattro:

- **La Virtualizzazione dei server,** che consente l'esecuzione congiunta di varie istanze di un sistema operativo su un singolo server. Questo modello rappresenta il modo migliore per aumentare l'utilizzo delle risorse, fino all'80% rispetto a un tasso di utilizzo medio del 10-20% dei comuni server fisici con un solo ruolo[1].
- **La virtualizzazione hardware dei server**, che fornisce solo un livello intermedio (hypervisor) tra la macchina virtuale (VM) e l'ambiente bare metal, offre un valore maggiore rispetto **virtualizzazione software dei server**, in cui il sistema operativo sottostante comporta un certo consumo di risorse aggiuntivo. Per le maggior parte delle applicazioni aziendali è pertanto preferibile la virtualizzazione hardware.
- **La virtualizzazione dei desktop,** che offre uno scenario di valore diverso con la sostituzione di una moltitudine di desktop fisici con un'infrastruttura desktop virtuale (**VDI**). "Thin client" convenienti dal punto di vista dei costi, desktop remoti basati sui ruoli, filiali remote senza bisogno di un servizio IT dedicato e tutta la gestione di centinaia di luoghi di lavoro limitata a un numero ridotto di server fisici.
- **La virtualizzazione delle applicazioni**, dove, a differenza dell'infrastruttura dei desktop remoti basati sui ruoli, viene adottato un ambiente virtuale solo per una singola applicazione. Per gli approcci Software-as-a-Service sempre più diffusi, questo modello rappresenta una scelta naturale ed efficiente.

Tutti i modelli di virtualizzazione hanno molteplici utilizzi e ogni utilizzo comporta alcuni rischi specifici. Tra questi, il rischio di minacce informatiche è uno dei più rilevanti e rende pertanto assolutamente necessaria l'adozione di una soluzione di sicurezza. Questo compito pone sfide ancora più complesse se si pensa che tutti questi tre approcci potrebbero essere impiegati all'interno di una singola rete IT. E occorre inoltre sostenere un ulteriore consumo di risorse.

Esistono in ogni caso alcuni modi per attenuare l'impatto sulla nuova infrastruttura virtuale ad alta efficienza.

---

1 Ruest D. Virtualization.A Beginners Guide. McGraw-Hill, 2010, pagina 4

UNA SOLUZIONE DI SICUREZZA SPECIALIZZATA PER GLI AMBIENTI VIRTUALI È ESSENZIALE

È ovviamente possibile installare i familiari agenti di protezione degli endpoint sulle macchine virtuali. Esistono però alcuni importanti punti di debolezza che possono rendere insoddisfacente l'esperienza con l'infrastruttura IT virtualizzata.

1. **Duplicazione.** Ogni VM avrà una serie identica di componenti per la sicurezza, tra cui un motore isolato anti-malware e i database delle firme, ognuno dei quali dovrà essere aggiornato in modo indipendente. Di conseguenza, una notevole parte delle preziose risorse, ad esempio potenza di elaborazione, RAM e archiviazione su disco, verrà consumata alquanto inutilmente, riducendo notevolmente il tasso di consolidamento risultante.

2. **"Storm".** Questo termine viene utilizzato per l'attività simultanea di scansione anti-malware o di aggiornamento dei database svolta da più macchine, la quale può causare un improvviso picco di consumo delle risorse con un conseguente calo delle prestazioni e persino una negazione del servizio. La configurazione manuale può aiutare parzialmente a risolvere il problema, ma, in caso di decine o centinaia di VM, l'intervento manuale potrebbe essere estremamente lungo.

3. **"Gap instant-on".** Alcune macchine virtuali restano inattive fino a quando non vengono chiamate in servizio quando ne sorge l'esigenza. Sfortunatamente non è possibile aggiornare i componenti o i database della soluzione di sicurezza su una VM inattiva. Immediatamente dopo l'avvio e prima del completamento dell'aggiornamento di sicurezza, la VM è pertanto vulnerabile agli attacchi.

4. **"Attacchi di panico".** È pratica comune tra gli amministratori di sistema predefinire la reazione a un'infezione da virus come una stretta dei parametri di sicurezza, con il passaggio alla modalità "paranoid" e l'attivazione di un processo di scansione non pianificato. Un tale criterio, che può avere senso per i nodi fisici, può facilmente portare a un insostenibile blocco dell'ambiente virtuale.

5. **Problemi di incompatibilità.** Le macchine virtuali sono per molti versi simili alle loro controparti fisiche, ma ci sono alcune importanti differenze da considerare, come l'utilizzo di dischi non persistenti o il processo di migrazione delle VM attive. Essendo stati progettati per gli endpoint fisici, gli anti-malware standard non tengono conto delle tante sfumature caratteristiche degli ambienti virtuali e possono quindi provocare rallentamenti e anomalie impreviste o persino non essere affatto eseguiti.

In considerazione di tutto quanto sopra, diventa ovvia l'esigenza generale di una soluzione specializzata. Tale prodotto dovrebbe essere creato tenendo conto di tutto quanto riportato in precedenza, fornendo al contempo il massimo livello possibile di protezione con il minimo impatto sulle prestazioni generali. Kaspersky Lab, il leader tecnologico mondiale nel campo della sicurezza informatica, è ben all'altezza del compito poiché offre una soluzione per le più diffuse piattaforme di virtualizzazione: VMware vSphere, Microsoft Hyper-V, Citrix XenServer e KVM.

PIATTAFORME E MODALITÀ DI PROTEZIONE

INTEGRAZIONE AGENTLESS CON VMWARE NSX

VMware, una delle prime piattaforme di virtualizzazione e tuttora la più diffusa, offre una nuova tecnologia che aiuta l'automazione degli ambienti virtuali VMware NSX. Questa tecnologia è un successore di vShield Endpoint, che consente di scaricare le macchine virtuali dal peso di sostenere database identici e di duplicare gli agenti di scansione anti-malware. Questo approccio viene definito "agentless".

Kaspersky Lab offre una soluzione di sicurezza specializzata per le piattaforme VMware: **Kaspersky Security for Virtualization | Agentless.** Con questa soluzione, le funzioni di scansione vengono trasferite a una singola SVM, una macchina virtuale specializzata che contiene sia il motore di scansione che i database della sicurezza, garantendo la protezione di tutte le macchine virtuali in esecuzione sull'hypervisor.

I vantaggi sono evidenti:

- **L'integrazione nativa con VMware NSX e vShield Endpoint** consente all'infrastruttura e ai livelli di sicurezza di funzionare insieme in stretta collaborazione, assicurando nuovi livelli di automazione e protezione ai data center software-defined.
- **L'implementazione automatizzata per VMware NSX** permette alla SVM di "apparire" automaticamente nell'hypervisor, in base ai requisiti delle macchine virtuali protette su tale host.
- **L'integrazione dei criteri di sicurezza** consente a ogni macchina virtuale di ricevere funzionalità di sicurezza precise, come definito dai criteri aziendali basati sui singoli ruoli delle macchine virtuali.
- **L'integrazione con i tag di sicurezza NSX** permette al data center software-defined di reagire in tempo reale agli incidenti, riconfigurando automaticamente l'intera infrastruttura virtuale, se necessario. Il supporto simultaneo per NSX e vShield Endpoint garantisce il completo allineamento delle strategie per la sicurezza e dell'IT ai bisogni aziendali.
- **Quando vengono avviate nuove macchine virtuali, la protezione viene fornita istantaneamente** tramite la SVM, senza "gap instant-on" o necessità di installare software aggiuntivo.
- **Il problema degli "storm" viene eliminato**, in quanto viene aggiornata una singola SVM, la quale esegue automaticamente la scansione delle macchine virtuali seguendo una pianificazione impostata casualmente e limitando il numero di thread utilizzati.

Inoltre, grazie all'aiuto delle funzioni base di sicurezza di rete fornite tramite la piattaforma NSX e la suite vCloud Networking and Security, la soluzione Kaspersky è in grado di rilevare e prevenire gli attacchi in ingresso sulle macchine virtuali, bloccando in modo efficiente l'autore dell'attacco mediante la tecnologia Network Attack Blocker[2].

Purtroppo le capacità di vShield Endpoint e NSX sono limitate, in quanto forniscono accesso alle macchine virtuali protette solo a livello di file system. I processi che avvengono all'interno della memoria delle VM non possono pertanto essere monitorate e controllate da un anti-malware agentless. Ciò significa inoltre che non è possibile implementare altre tecnologie di protezione degli endpoint, come Application Control con whitelisting dinamico, progettate per fornire ulteriori e potenti livelli di sicurezza.

Occorre anche notare che, poiché vShield Endpoint e NSX sono tecnologie proprietarie di VMware, il principio agentless per la sicurezza di un'infrastruttura virtuale può essere applicato al momento solo alla piattaforma VMware.

---

2 La configurazione della protezione di rete in KSV | Agentless richiede l'implementazione di una seconda SVM

LIGHT AGENT PER QUALSIASI PIATTAFORMA DI VIRTUALIZZAZIONE

Consapevole delle limitazioni descritte sopra, **Kaspersky Lab** offre un'altra variante della soluzione per la virtualizzazione, un approccio che si pone a metà strada tra l'opzione agentless e full agent: **Kaspersky Security for Virtualization | Light Agent**.

Come per l'approccio agentless, i database e il motore anti-malware per la scansione dei file vengono collocati nella SVM, ma con una differenza: su ogni VM da proteggere viene implementato un modulo residente leggero.

Grazie allo sviluppo interno, Kaspersky Security for Virtualization | Light Agent non è limitato dalle capacità di nessuna piattaforma di virtualizzazione, ma dispone di accesso diretto completo a ogni macchina virtuale, nonché a ciò che accade all'interno di ogni memoria operativa. Di conseguenza, è possibile utilizzare la gamma completa di tecnologie all'avanguardia di Kaspersky Lab per difendere l'infrastruttura virtualizzata.

I vantaggi principali di Kaspersky Security for Virtualization | Light Agent includono:

- **Minore consumo di risorse** rispetto alla soluzione full agent, poiché il motore di scansione dei file system e i database sono trasferiti alla SVM dedicata.
- **Supporto delle piattaforme di virtualizzazione più diffuse:** VMware vSphere con NSX, Microsoft Hyper-V, Citrix XenServer e KVM.
- **Il più alto livello possibile di protezione**, reso possibile dall'acceso completo alle risorse delle VM, inclusa la memoria operativa.
- **Diventano disponibili ulteriori livelli di sicurezza proattiva**, come i sistemi di prevenzione delle intrusioni basata su host (HIPS) dotati di tecnologia di prevenzione automatica degli exploit (AEP) e Application Control con whitelisting dinamico. Possono essere implementati con facilità anche gli scenari di sicurezza più stringenti, tra cui un criterio "Default Deny".
- **Essendo stata progettata dall'inizio per la virtualizzazione**, la soluzione opera congiuntamente alle funzionalità uniche dell'ambiente virtuale, non in contrasto con esse.

Ovviamente, tutto ha un prezzo. Il Light Agent deve essere presente su ogni nuova VM implementata, un processo che può essere facilmente automatizzato includendolo nell'immagine VM pregenerata. A causa della presenza del Light Agent stesso, Kaspersky Security for Virtualization | Light Agent occupa una quantità di memoria alquanto maggiore rispetto all'applicazione agentless, ma va detto che, in determinate condizioni, la soluzione Light Agent può effettivamente essere più veloce delle soluzioni di sicurezza agentless basate su NSX e vShield che forniscono soltanto protezione a livello di file alle macchine virtuali.

Un altro aspetto da ricordare è che il numero di hypervisor supportati è limitato dalle tre piattaforme più diffuse. Inoltre, al momento della redazione del presente documento, la famiglia Microsoft Windows è l'unico sistema operativo ospite supportato dalle applicazioni Agentless e Light Agent.

Ma ciò certamente non significa essere senza difesa se non si utilizza una di queste tre piattaforme. C'è ancora da considerare una sicurezza full agent, progettata da Kaspersky Lab.

APPROCCIO FULL AGENT

Kaspersky Endpoint Security, nonostante sia una soluzione full agent, è di fatto in grado di svolgere un ottimo lavoro negli ambienti virtuali. Anche se richiede più risorse di Kaspersky Security for Virtualization, può essere adottata per l'utilizzo negli ambienti virtuali. Se pertanto occorre proteggere una configurazione particolare, che si tratti di una serie di server Linux o di ospiti Windows su qualche hypervisor meno diffuso, è comunque disponibile una soluzione.

I vantaggi dell'implementazione di Kaspersky Endpoint Security su una infrastruttura virtuale includono:

- Supporto dei sistemi operativi più moderni
- Integrazione della serie più completa di tecnologie avanzate di Kaspersky Lab
- Principi di gestione assolutamente familiari, come per qualsiasi normale macchina fisica
- Efficienza riconosciuta dalle tre principali società di consulenza del mondo Gartner, IDC e Forrester, dalle quali è stata nominata una delle migliori piattaforme disponibili per la protezione degli endpoint: una "triplice corona".

Tabella 1: elenco comparativo delle funzioni

Funzione	Kaspersky Security for Virtualization | Agentless	Kaspersky Security for Virtualization | Light Agent	Kaspersky Endpoint Security for Business
Piattaforme di virtualizzazione supportate	VMware vSphere con NSX	VMware vSphere, Microsoft Hyper-V, Citrix XenServer e KVM	Tutte eccetto quelle a livello di sistema operativo[3]
Sistema operativo ospite supportato	MS Windows	MS Windows	MS Windows, Mac OS X, Linux
Mantenimento dei tassi di consolidamento	+	+	-
Gestione centralizzata tramite Kaspersky Security Center	+	+	+
Funzionalità KSN	+	+	+
Protezione di nuove VM senza installazioni aggiuntive	+	+/-[4]	-
Motore anti-malware	+	+	+
Ridondanza per il motore anti-malware	-	+	-
System Watcher per proteggere la memoria e i processi	-	+	+
Prevenzione delle intrusioni basata su host (HIPS)	-	+	+
Network Attack Blocker	+	+	+
Application Control con whitelisting dinamico e supporto del criterio Default Deny	-	+	+
Web Control	-	+	+
Device Control	-	+	+
System Management	-	+[5]	+[5]
Crittografia	-	-	+

Dopo tutti i noiosi calcoli, si pone ancora una volta la domanda: come ottenere la massima efficienza senza diventare vulnerabili alle minacce informatiche? Esiste un approccio che può essere considerato come principio generale e che viene definito **sicurezza basata sui ruoli.**

3 La virtualizzazione a livello di sistema operativo, detta anche "basata su aree" o "basata su contenitori", impiega un meccanismo in cui molti contenitori dell'area utenti condividono un singolo kernel del sistema operativo. Parallels e Proxmox sono esempi di piattaforme di questo tipo.

4 Per le macchine virtuali non persistenti, la protezione istantanea è disponibile dopo l'inclusione del Light Agent nell'immagine della macchina virtuale. Per le VM persistenti, l'amministratore deve implementare il Light Agent manualmente.

5 La tecnologia di valutazione delle vulnerabilità/gestione delle patch, pur essendo disponibile in Kaspersky Security for Virtualization | Light Agent, richiede un elevato utilizzo di risorse e pertanto non se ne consiglia l'implementazione negli ambienti virtuali.

PARARE SOLO I COLPI IN ARRIVO: APPROCCIO ALLA SICUREZZA BASATO SUI RUOLI

Ogni minaccia informatica che attenta agli endpoint fisici può mettere a repentaglio anche l'infrastruttura virtuale. Ma ciò che è assolutamente necessario all'autore di un attacco è un metodo che gli consenta di penetrare nel perimetro di sicurezza dell'azienda per eseguire l'attacco. Ad esempio, per infettare un PC, un cybercriminale potrebbe attirare il dipendente a un sito dannoso, dove avviene l'infezione sfruttando una vulnerabilità presente nel browser della vittima. Ma per infettare, ad esempio, un server di database nascosto in profondità nell'infrastruttura IT che potrebbe anche non disporre di connettività Internet, occorre trovare un altro vettore di attacco. Pertanto, se si è certi che le sole minacce possibili sono quelle rivolte a livello di file system o che i dati in questione sono di basso valore oppure se si utilizza un'infrastruttura VDI strettamente controllata senza accesso al Web, si può optare per una soluzione agentless che offre i vantaggi di una protezione istantanea, senza "gap instant-on".

Tabella 2: approccio alla sicurezza basato sui ruoli

Ruolo	Accesso esterno	Valore dei dati	Valore del servizio	Condizioni esterne	Soluzione (motivo del suo utilizzo)
Server di database back-end	No	Da basso a medio	Da medio ad alto	Backup regolari	KSV | Agentless (dati di breve durata, meno vettori di attacco)
Server Web front-end	Sì	Basso	Alto	Hanno relazioni di trust con vari back-end	KSV | Light Agent (esposizione a pericoli di accesso pubblico, dopo un attacco riuscito è possibile lo sfruttamento dei trust)
VDI o applicazione virtualizzata a scopo limitato	No	Da medio ad alto	Medio	Con restrizioni elevate, nessuna installazione di app, nessun utilizzo di dispositivi di archiviazione rimovibili	KSV | Agentless (ambiente prevedibile, meno vettori di attacco)
Infrastruttura VDI sostitutiva dei desktop	Sì	Medio	Medio	Utilizzo di dispositivi di archiviazione rimovibili, utenti con diritti di installazione	KSV | Light Agent (l'esigenza di una sicurezza più elevata è maggiore rispetto all'esigenza di una risposta più rapida. Più vettori di attacco a causa dell'esposizione a Internet pubblico)
Server Web dell'Intranet aziendale	Sì	Da basso a medio	Da basso a medio	Accesso esterno consentito solo a utenti autorizzati mediante token hardware	KSV | Agentless (basso valore dei dati per l'azienda, esposizione molto limitata a Internet pubblico)
Infrastruttura di elaborazione dati client	Sì	Alto	Alto	Esigenza di un ambiente stabile e invariato; consigliato Application Control con Default Deny	KSV | Light Agent (l'esigenza di conformità rende assolutamente necessari livelli di protezione aggiuntivi)
Infrastruttura di test per gli sviluppatori Web	Sì	Da basso a medio	Medio	Hypervisor basato su Linux e VM ospiti eterogenee	KESB for Linux, KESB for Windows (dati di breve durata costantemente rinnovati, varietà di sistemi operativi)

La tabella contiene alcuni esempi che offrono un quadro generale delle difese basate sui ruoli. Tuttavia, per rendere più chiaro il concetto, di seguito è riportata più dettagliatamente la classificazione relativa a Valore dei dati e Valore del servizio:

- **Dati con valore basso:** questi dati sono solitamente spersonalizzati, non contengono segreti personali, commerciali o governativi preziosi, sono probabilmente di breve durata e soggetti a costante rinnovo. La loro perdita o la loro esposizione non comporta perdite significative dal punto di vista commerciale e non può mai causare danni alla reputazione. Un valido esempio può essere rappresentato da un database operativo in cui vengono temporaneamente archiviati dati transitori.
- **Dati con valore medio:** questi dati possono contenere alcune informazioni personali o commerciali, ad eccezione di quelle direttamente connesse ad aspetti finanziari e al benessere personale. Non dovrebbero contenere informazioni classificate come riservate La loro perdita può causare danni finanziari all'azienda. La loro esposizione può comportare notevoli conseguenze sotto il profilo monetario e può danneggiare la reputazione dell'azienda in modo non critico. Esempio: dati sui clienti di un rivenditore che opera tramite Internet.
- **Dati con valore alto:** possono contenere informazioni personali e/o finanziarie sensibili o segreti commerciali che costituiscono una parte importante del vantaggio competitivo dell'azienda. Possono inoltre contenere informazioni classificate come riservate. La loro perdita può provocare perdite commerciali o alla reputazione. La loro esposizione può comportare pesanti sanzioni finanziarie, comprese azioni legali, e danni irrimediabili alla reputazione. Esempio: piani relativi a infrastrutture critiche o corrispondenza riservata a livello dirigenziale.
- **Servizio con valore basso:** nessuna terza parte ne è interessata, la velocità di ripristino è di scarsa importanza. Scarsa o nessuna conseguenza finanziaria in caso di suo malfunzionamento. La probabilità di danni alla reputazione è estremamente bassa. Esempio: portale informativo aziendale.
- **Servizio con valore medio:** ne sono interessate terze parti in caso di malfunzionamento del servizio. La perdita di tali dati può comportare notevoli danni finanziari. Anche i danni alla reputazione sono notevoli e sono direttamente connessi alla rilevanza sociale del servizio: quanto più il servizio (o un prodotto che basa su di esso) è conosciuto e popolare, tanto più pesanti sono le conseguenze per la reputazione. I dati possono far parte di un'infrastruttura governativa, ma le loro condizioni hanno scarsa influenza sul benessere nazionale. Il ripristino rapido è di primaria importanza. Esempio: infrastruttura VDI di un integratore di sistemi che fornisce, tra i suoi servizi, un ambiente sostitutivo dei desktop.
- **Servizio con valore alto:** quasi certamente ne sono interessate terze parti. Il servizio è l'elemento chiave dell'attività e può essere anche un elemento critico dell'attività di terze parti. È possibile un'influenza sul benessere nazionale. Le perdite di reputazione sono estremamente elevate e potrebbero essere irrimediabili. Il ripristino è di massima importanza. Il mancato ripristino nel più breve tempo possibile può provocare ulteriori conseguenze gravi. Esempio: infrastruttura di sistemi di videosorveglianza governativi.

Va però ricordato che, prima di implementare una qualsiasi soluzione di sicurezza specializzata, è consigliabile verificare e regolare le impostazioni di sicurezza di base della rete IT. Una rete amministrata correttamente significa meno vettori di attacco per i criminali e meno conseguenze nel caso in cui qualcosa vada male.

L'EFFICIENZA SI TRADUCE IN INTEGRITÀ

L'utilizzo efficiente delle risorse è un bene, ma non è nulla senza un controllo efficace. È certamente possibile implementare una soluzione agentless di un fornitore per i back-end, una soluzione light-agent di un altro per l'infrastruttura VDI e utilizzare il controllo delle applicazioni di una terza parte per un'area critica. In questo caso, si avranno tre console di gestione, tre serie di criteri da configurare e gestire e un traffico di aggiornamento eccessivo da immettere nel canale dei dati. È senz'altro molto meglio che tutto provenga da un singolo fornitore, con tutte le funzionalità di misurazione e controllo organizzate in modo chiaro all'interno di una singola console. Tutti i prodotti Kaspersky Security sono progettati per essere controllati a livello centrale tramite Kaspersky Security Center. Ciò significa che è possibile gestire le risorse virtualizzate dalla stessa console utilizzata per controllare la sicurezza degli endpoint fisici.

Un altro vantaggio è rappresentato dall'aggiornamento centralizzato. Non c'è bisogno di scaricare la stessa serie di aggiornamenti per ogni SVM su ogni hypervisor, poiché vengono implementati automaticamente dopo essere stati scaricati nell'archivio di Kaspersky Security Center (KSC).

Un'altra caratteristica distintiva delle soluzioni di Kaspersky Lab è la loro disponibilità per piattaforme di virtualizzazione differenti. È pertanto possibile utilizzare un ambiente multi-hypervisor ben protetto e comunque usufruire di tutti i controlli riuniti all'interno dello stesso KSC.

Ad esempio, gli elementi core di Active Directory (controller di dominio, Domain Name System e così via) possono essere ospitati sui server virtuali Microsoft Hyper-V, utilizzare un'infrastruttura VDI basata su Citrix e includere server di database in esecuzione su VMware vSphere. Oppure, come illustrato nella figura precedente, è possibile utilizzare un ambiente misto contenente più di una piattaforma di hypervisor ed endpoint fisici.

In questo caso, per ottenere l'equilibrio più efficiente tra prestazioni e sicurezza e di conseguenza tassi di consolidamento ottimali:

- L'infrastruttura server critica per l'azienda e contenente dati preziosi dovrebbe essere protetta tramite gli alti livelli di sicurezza di KSV | Light Agent, Tuttavia, per le infrastrutture basate su VMware (soprattutto per quelle in possesso della piattaforma VMware NSX), è possibile prendere in considerazione anche una soluzione agentless.
- Le infrastrutture desktop virtuali in rapida crescita, contenenti utenti regolari, dovrebbero essere protette solo da KSV | Light Agent. L'ambiente di test, che comprende un sistema operativo Linux ed endpoint fisici, viene protetto meglio da Kaspersky Endpoint Security.

In ogni caso, i prodotti Kaspersky Lab forniscono la migliore protezione che il settore ha da offrire e consentono di scegliere tra la facile implementazione e l'efficienza del ROI della soluzione KSV | Agentless, l'alto livello di protezione di KSV | Light Agent o una qualsiasi combinazione all'interno di una singola infrastruttura IT.

Poiché Kaspersky Lab offre ai clienti una sicurezza agentless, light agent e agent-based per le implementazioni virtualizzate, siamo in grado di fornire ai nostri clienti consigli assolutamente obiettivi. Non sentiamo di dover promuovere una tecnologia in particolare, ma possiamo individuare la scelta migliore o una combinazione di opzioni per l'ambiente specifico del cliente. Inoltre, poiché tutte le nostre soluzioni sono basate sullo stesso potente motore anti-malware e sono da noi progettate come parte di un'unica piattaforma di sicurezza integrata, sappiamo che qualunque decisione del cliente funzionerà in modo efficiente per mantenere protetto il sistema virtuale.

www.kaspersky.it

Twitter.com/
KasperskyLabIT

Facebook.com/
Kasperskylabitalia

Youtube.com/
Kasperskyitalia

KASPERSKY lab

Tutto sulla sicurezza in Internet: **www.securelist.com**
Trovate il partner più vicino: **www.kaspersky.it/buyoffline**