SEGURANÇA DE VIRTUALIZAÇÃO: COMPREENDER A DIFERENÇA

Kaspersky Security for Virtualization

KASPERSKY lab

Segurança de virtualização: compreender a diferença

Já está a converter os seus ativos de hardware para ativos virtuais? Então, o objetivo da sua empresa é quase de certeza obter a eficiência máxima da infraestrutura de TI. A execução de várias máquinas virtuais (VM) num único computador, em que todas elas requerem alimentação, refrigeração e manutenção próprias, em vez da utilização de servidores dedicados, é um argumento convincente. A utilização de vários nós virtualizados alimentados por um único servidor físico permite que a empresa reduza os custos. O impacto económico da virtualização pode ser surpreendentemente poderoso: de acordo com um inquérito realizado pela Forrester em 2011, a implementação de uma infraestrutura VMware VDI correspondeu a 255% do ROI ajustado em função do risco num período de 4 anos, tendo atingido o ponto de equilíbrio 17 meses após a implementação.

A questão é, quantas VM pode implementar na sua configuração de hardware sem verificar um impacto significativo no desempenho? Tal é conhecido como "taxa de consolidação" e esta é a parte mais complicada, sendo necessário considerar um grande número de fatores. Que tipos de tarefas devem efetuar as máquinas virtuais? Que tipo de software hipervisor utiliza? Quais são os riscos de colocar todos os ovos no mesmo cesto? E como pode colocar a sua nova infraestrutura virtual em segurança, certificando-se de que não está vulnerável a cibercriminosos, sem tomar atitudes extremas e sem tornar tudo extremamente lento? Para tomar a decisão certa, é necessário compreender vários conceitos e analisar como funcionam em conjunto.

Modelos de virtualização

A indústria definiu vários modelos de virtualização. Este documento considera três modelos:

- **Virtualização de servidores** –permitindo que várias instâncias de um sistema operativo sejam executadas num único servidor. Esta é a melhor forma de aumentar a utilização de recursos – até 80% em comparação com a taxa de utilização média de 10-20% para servidores físicos comuns com uma única função[1]. **Virtualização de servidor de hardware**, existindo apenas uma camada intermédia (hipervisor) entre a máquina virtual (VM) e o metal, que representa um valor superior do que a **Virtualização de servidor de software**, em que o sistema operativo subjacente envolve um consumo adicional de recursos. Assim, a Virtualização de hardware é a solução preferencial para a maior parte das aplicações empresariais.
- **Virtualização de ambiente de trabalho** - oferece um cenário com um valor diferente, substituindo um grande número de ambientes de trabalho físicos com a Infraestrutura de computadores pessoais virtuais (**VDI**). "Clientes magros" rentáveis, ambientes de trabalho remotos com base na função, ramos remotos sem necessidade de um serviço de TI dedicado e todo o trabalho de manutenção de centenas de locais de trabalho, limitados a meia dúzia de servidores físicos.
- **Virtualização de aplicações** - aqui, ao contrário do que acontece numa infraestrutura de ambiente de trabalho remoto com base na função, é adotado um ambiente virtual apenas para uma única aplicação. Esta é uma escolha natural e eficiente para as abordagens de software enquanto serviço cada vez mais populares.

Todos os modelos de virtualização têm muitas utilizações e cada utilização envolve alguns riscos relevantes. Entre estes, o risco de ciberameaças é um dos mais significativos, fazendo com que seja absolutamente necessário implementar algum tipo de solução de segurança. Esta tarefa torna-se ainda mais difícil quando se tiver em conta que é possível utilizar todas as três abordagens numa única rede de TI. E, sim, também é necessário lidar com o consumo adicional de recursos.

---

[1] - *Ruest D. Virtualization. A Beginners Guide. McGraw-Hill, 2010, página 4*

No entanto, existem formas de reduzir o impacto na sua recém-criada infraestrutura virtual de elevada eficiência.

É essencial uma solução de segurança especializada para ambientes virtuais

É evidente que pode instalar os agentes Endpoint Protection que já conhece nas suas máquinas virtuais. Mas a verdade é que existem algumas lacunas que podem tornar a sua experiência com uma infraestrutura de TI virtualizada insatisfatória.

1. **Duplicação**. Cada VM tem um conjunto idêntico de componentes de segurança, incluindo um motor anti-malware e bases de dados de assinaturas, e cada conjunto tem de ser atualizado de forma independente. Como tal, uma parte significativa dos seus valiosos recursos – capacidade de processamento, RAM e armazenamento em disco – é consumida inutilmente, reduzindo significativamente a taxa de consolidação resultante.
2. "**Surtos**". Este termo é utilizado para verificação anti-malware simultânea ou atualização de bases de dados por várias máquinas, o que pode originar um pico repentino no consumo de recursos e a consequente redução do desempenho e até mesmo a uma recusa de serviço. A configuração manual pode ajudar a resolver parcialmente esta questão, mas a intervenção manual pode ser extremamente demorada devido às classificações e às centenas de VM.
3. "**Falha instantânea**". Algumas máquinas virtuais permanecem inativas até ser necessária a sua ativação. Infelizmente, não é possível atualizar componentes da solução de segurança ou bases de dados numa VM inativa. Portanto, imediatamente após a inicialização e antes da conclusão da atualização de segurança, a VM está vulnerável a um ataque.
4. **"Ataques de pânico".** Trata-se de uma prática comum entre administradores de sistemas para predefinir a reação a um surto de vírus como um reforço dos parâmetros de segurança, passando para o modo "paranoid" e ativando um processo de verificação não programado. Este tipo de política, que pode ser importante para nós físicos, pode causar facilmente a paralisação de um ambiente virtual.
5. **Problemas de incompatibilidade.** As máquinas virtuais são em muitos aspetos semelhantes aos seus equivalentes físicos, mas existem grandes diferenças a ter em atenção, como a utilização de discos não permanentes ou o processo de migração VM em tempo real. O anti--malware padrão, uma vez que foi concebido para terminais físicos, não tem em conta as muitas nuances características dos ambientes virtuais, pelo que pode causar atrasos e falhas técnicas ou mesmo o não funcionamento.

Face ao exposto, a necessidade global de uma solução especializada torna-se óbvia. Este tipo de produto deve ser criado tendo todas as considerações acima indicadas em mente, proporcionando o mais elevado nível de proteção possível com o mínimo impacto no desempenho global. A Kaspersky Lab, líder em tecnologia a nível mundial no campo da cibersegurança, está preparada para a tarefa, oferecendo uma solução para as três plataformas de virtualização mais populares – VMware, Microsoft Hyper-V e Citrix.

Plataformas e modos de proteção

Abordagem Agentless

A VMware, uma das mais antigas e a mais popular plataforma de virtualização, fornece uma solução denominada vShield, que permite aliviar a sobrecarga de bases de dados idênticas e agentes duplicados de verificação anti-malware da VM. É denominada abordagem "Agentless".

A Kaspersky Lab oferece uma solução de segurança especializada para plataformas VMware, o **Kaspersky Security for Virtualization | Agentless.** As funções de verificação são transferidas para um único equipamento virtual de segurança (SVA), uma máquina virtual especializada que contém o motor de verificação e as bases de dados de segurança, protegendo todas as VM em execução no hipervisor.

As vantagens são claras:

- A interface nativa fornecida pela solução VMware vShield oferece um acesso eficiente a VM, libertando os recursos das máquinas individuais e garantindo a compatibilidade com outras tecnologias VMware
- Os recursos libertados devido à concentração das funções anti-malware e a base de dados de assinatura num único equipamento virtual podem agora ser utilizados para implementar VM adicionais, aumentando a taxa de consolidação.
- À medida que as novas VM são iniciadas, o SVA fica protegido de imediato, sem "falhas instantâneas" e sem que seja necessário instalar qualquer software adicional.
- O SVA da Kaspersky sempre alerta mantém a respetiva base de dados de assinatura sempre atualizada e, ainda mais importante, mantém a ligação ao Kaspersky Security Network (KSN), uma infraestrutura a nível mundial que processa informações de milhões de participantes voluntários e fornece proteção contra as ameaças mais recentes mesmo antes de serem implementadas através das atualizações da base de dados.
- O problema de "surtos" é erradicado, uma vez que é atualizado um único SVA, o qual, verifica automaticamente as VM, seguindo uma ordem definida aleatoriamente e limitando o número de threads utilizadas.

Além disso, com a ajuda das funções básicas de segurança da rede fornecidas através do vCloud Networking and Security, a solução da Kaspersky consegue detetar e evitar ataques aos VM, bloqueando eficazmente o autor do ataque com a tecnologia Bloqueador de ataques de rede[1].

Infelizmente, as capacidades da solução vShield são limitadas, permitindo o acesso a VM protegidas apenas ao nível de sistemas de ficheiros. Assim, os processos que ocorrem na própria memória da VM não podem ser monitorizados e controlados por anti-malware Agentless. Isto também significa que não é possível implementar outras tecnologias de proteção de terminais, como o Controlo de aplicações com listas brancas dinâmicas, concebidas para fornecer poderosas camadas adicionais de segurança.

É importante salientar que atualmente, dado que a solução vShield é uma tecnologia VMware, o princípio Agentless para a segurança de uma infraestrutura virtual também só pode ser aplicado à plataforma VMware.

Abordagem Light Agent

Consciente das limitações acima referidas, a **Kaspersky Lab** oferece uma outra versão da solução de virtualização. Uma abordagem que se situa entre a abordagem Agentless e Full Agent: **Kaspersky Security for Virtualization | Light Agent**.

Tal como acontece com a abordagem Agentless, as bases de dados e o motor anti-malware de verificação de ficheiros estão localizados no SVA. Mas há uma diferença: é implementado um módulo residente lightweight em cada VM protegida.

O Kaspersky Security for Virtualization | Light Agent não é limitado pelas capacidades de segurança da tecnologia vShield, mas tem acesso direto a cada VM, incluindo tudo o que está a acontecer em cada memória operativa. Como tal, é possível implementar a gama completa de tecnologias inovadoras da Kaspersky Lab para defender a infraestrutura virtualizada.

As principais vantagens do Kaspersky Security for Virtualization | Light Agent incluem:

- Menos consumo de recursos em comparação com uma solução baseada em Full Agent, uma vez que o motor de verificação de sistemas de ficheiros e as bases de dados são transferidos para o SVA dedicado.
- Suporta as três plataformas de virtualização mais populares – VMware, Microsoft Hyper-V e Citrix*
- O nível mais elevado de proteção possível, através do acesso total aos recursos da VM, incluindo a memória operativa.
- Ficam disponíveis camadas de segurança pró-ativas adicionais, como HIPS com Prevenção automática de exploit e Controlo de aplicações com listas brancas dinâmicas. É fácil implementar, mesmo nos cenários de segurança mais rigorosos, incluindo "Negação predefinida".
- Inicialmente concebida a pensar na virtualização, a solução funciona com as funcionalidades exclusivas do ambiente virtual, não em conflito com as mesmas.

Obviamente, tudo tem um preço. O Light Agent tem de estar presente em todas as VM recém--implementadas – um processo facilmente automatizado, incluindo o LA, na imagem VM pré-gerada. Devido à presença do próprio Light Agent, o Kaspersky Security for Virtualization | Light Agent tem um impacto relativamente maior na memória do que a aplicação Agentless; mas, é importante salientar que, em determinadas condições, a solução Light Agent pode ultrapassar a aplicação Agentless com base em vShield.

Outro facto que convém lembrar é que o número de hipervisores suportados é limitado pelas três plataformas mais populares. Além disso, quando este documento foi redigido, a família Microsoft Windows era o único SO convidado suportado pelas aplicações Agentless e Light Agent.

Mas é óbvio que isto não significa que não está protegido caso não implemente uma destas três plataformas. Há ainda a considerar a segurança com base em Full Agent, concebida pela Kaspersky Lab.

Abordagem Full Agent

Embora seja uma segurança Full Agent, o **Kaspersky Endpoint Security** é, na realidade, capaz de efetuar um bom trabalho em ambientes virtuais. Embora exija mais recursos do que o Kaspersky Security for Virtualization, pode ser adotado para utilização em ambientes virtuais. Portanto, continua protegido caso seja necessário proteger uma configuração peculiar, quer seja um conjunto de servidores Linux ou de convidados Windows num hipervisor exótico.

As vantagens da implementação do Kaspersky Endpoint Security na sua infraestrutura virtual incluem:

- Suporta a maioria dos sistemas operativos atuais
- Integra o conjunto mais abrangente de tecnologias avançadas da Kaspersky Lab
- Princípios de gestão com os quais está totalmente familiarizado, tal como qualquer máquina física normal
- A sua eficácia é reconhecida por três das agências de consultoria líderes a nível mundial, a Gartner, a IDC e a Forrester, tendo sido considerada uma das melhores plataformas de proteção de terminais; uma "tripla coroa".

---

1 A configuração de proteção da rede no KSV | Agentless requer a implementação de um SVA secundário

Tabela 1: Lista comparativa de funcionalidades

Funcionalidade	Kaspersky Security for Virtualization | Agentless	Kaspersky Security for Virtualization | Light Agent	Kaspersky Endpoint Security for Business
Plataformas de virtualização suportadas	VMware	VMware, Microsoft Hyper-V, Citrix	Qualquer uma, exceto SO de nível[1]
SO convidado suportado	MS Windows	MS Windows	MS Windows, Mac OS X, Linux
Taxa de consolidação num único anfitrião	* * *	* */* * *[2]	*
Gestão centralizada através do Kaspersky Security Center	+	+	+
Funcionalidade KSN	+	+	+
Proteção de novas VM sem instalações adicionais	+	+/-[3]	-
Anti-malware	* *	* * *	* * *
Firewall	-	+	+
Prevenção de invasão com base em anfitrião (HIPS)	-	+	+
Bloqueador de Ataques de Rede	+	+	+
Controlo de aplicações com listas brancas dinâmicas e suporte para Negação predefinida	-	+	+
Controlo Web	-	+	+
Controlo de Dispositivos	-	+	+
Gestão de Sistemas	-	+[4]	+[4]
Encriptação	-	-	+

Assim, após todos os cálculos maçadores, a questão coloca-se novamente: como obter a máxima eficiência sem ficar vulnerável a ciberameaças? Existe uma abordagem que pode ser utilizada como regra geral e é designada por **segurança baseada em funções**.

---

[1] – A virtualização a nível do SO, também denominada baseada em zonas ou baseada em contentores, utiliza um mecanismo em que muitos "contentores" do espaço do utilizador partilham um único kernel do SO. O Parallels e o Proxmox são exemplos dessas plataformas.

[2] – Depende do hipervisor e do tipo de virtualização.

[3] – Para VM não persistentes, está disponível a proteção instantânea após incluir um Light Agent na imagem da VM. Para VM persistentes, o administrador tem de implementar um LA manualmente.

[4] – A tecnologia de Avaliação de vulnerabilidades/Gestão de patches, disponível nominalmente no Kaspersky Security for Virtualization | Light Agent, exige muitos recursos e, assim, a sua implementação em ambientes virtuais não é recomendada.

Apenas evita os ataques; uma abordagem à segurança baseada em funções.

Todas as ciberameaças aos terminais físicos também podem ameaçar a sua infraestrutura virtual. Mas o que é absolutamente necessário para a realização de um ataque, é um método de infiltração no seu perímetro de segurança. Por exemplo, ao infetar um PC em funcionamento, o cibercriminoso pode ter de atrair o colaborador para o website malicioso, onde ocorre a infeção através da exploração da vulnerabilidade do browser da vítima. Mas para infetar, por exemplo, um servidor de base de dados que esteja oculto na infraestrutura de TI e que possa até não ter ligação à Internet, é necessário encontrar outro vetor de ataque. Por conseguinte, se tiver a certeza de que as únicas ameaças possíveis são as que atacam a nível do sistema de ficheiros ou que os dados em questão têm pouco valor por si só, ou se estiver a utilizar uma VDI controlada com rigor sem aceder à Web, pode optar por uma solução Agentless que oferece as vantagens de proteção imediata sem "falhas instantâneas".

Tabela 2: Abordagem de segurança baseada em funções

Função	Acesso externo	Valor de dados*	Valor de serviço**	Condições ext.	Solução (Porque é que deve ser utilizada uma determinada solução)
Servidores de base de dados back-end	Não	Baixo a médio	Médio a alto	Cópias de segurança regulares	KSV | Agentless (dados de curta duração, menos vetores de ataque)
Servidores Web front-end	Sim	Baixo	Alto	Ter relações de fidedignidade com vários back-ends	KSV | Light Agent (Exposto aos perigos de acesso público; é possível a exploração de fidedignidades após um ataque com êxito)
VDI com finalidade limitada ou aplicação virtualizada	Não	Médio a alto	Médio	Extremamente restrito, sem instalação de aplicações, sem utilização de armazenamento amovível	KSV | Agentless (ambiente previsível, menos vetores de ataque)
VDI de substituição de ambiente de trabalho	Sim	Médio	Médio	Armazenamento amovível pessoal em utilização, utilizadores privilegiados com direitos de instalação	KSV | Light Agent (A necessidade de um nível de proteção superior é maior do que a necessidade de uma resposta mais rápida. Mais vetores de ataque devido à exposição à Internet pública)
Servidores de intranet empresariais	Sim	Baixo a médio	Baixo a médio	*Acesso externo apenas de utilizadores autorizados através de tokens de hardware	KSV | Agentless (Dados com pouco valor empresarial, exposição muito limitada à Internet pública)

Infraestrutura de processamento de dados de clientes	Sim	Alto	Alto	Necessidade de um ambiente estável e inalterado; recomendado Controlo de aplicações com negação predefinida	KSV | Light Agent (O requisito de conformidade torna as camadas de proteção adicionais uma necessidade indispensável.)
Infraestrutura de teste de desenvolvimento Web	Sim	Baixo a médio	Médio	Hipervisor baseado em Linux e VM convidadas heterogéneas	KESB para Linux, KESB para Windows (dados de curta duração renovados constantemente, vários SO)

A tabela acima contém alguns exemplos que fornecem uma perspetiva geral das defesas baseadas em funções, pelo que não são uma recomendação direta para as funções listadas e não devem ser utilizados dessa forma. Cada caso de utilização é único; existem sempre mais condições a ter em conta do que as que podem ser resumidas numa tabela. No entanto, para tornar o conceito mais claro, gostaríamos de apresentar a classificação para o Valor de dados e Valor de serviço mais pormenorizadamente:

- **Dados de baixo valor** – Estes dados são geralmente anónimos, não contêm segredos pessoais, comerciais ou governamentais valiosos e é possível que sejam de curta duração e sujeitos a constante renovação. A sua perda ou exposição não provoca perdas comerciais significativas e não causa danos à reputação. Um bom exemplo seria uma base de dados onde são armazenados temporariamente dados de transição.
- **Dados de valor médio** – Estes dados podem conter algumas informações pessoais ou comerciais com a exceção de dados diretamente relacionados com finanças e bem-estar pessoal. Não contêm informações confidenciais. A sua perda pode causar alguns danos financeiros à empresa. A sua exposição pode ter um impacto monetário considerável e pode prejudicar a reputação da empresa sem consequências graves. Exemplo – dados sobre os clientes de um revendedor na Internet.
- **Dados de elevado valor** – Podem conter informações pessoais e/ou financeiras confidenciais ou segredos comerciais que constituem uma parte significativa da vantagem competitiva da empresa no mercado. Também podem conter informações confidenciais. A sua perda pode resultar em perdas comerciais e danos à reputação significativos. A sua exposição pode levar a sanções financeiras pesadas, incluindo processos judiciais e danos irreversíveis à reputação. Exemplo – planos de uma infraestrutura crítica ou correspondência confidencial a um nível executivo.
- **Baixo valor de serviço** - Terceiros não afetados; rapidez de recuperação pouco significativa. Poucas ou nenhumas consequências financeiras em caso de mau funcionamento. A probabilidade de danos à reputação é extremamente baixa. Exemplo – portal de informações empresariais.
- **Valor médio de serviço** – Possibilidade de afetar terceiros em caso de mau funcionamento do serviço. A perda desses dados pode levar a prejuízos financeiros relevantes. Os danos à reputação são também consideráveis e estão relacionados diretamente com a importância social do serviço: quanto mais conhecido e popular for o serviço (ou o produto), maiores são as consequências ao nível da reputação. Os dados podem ser parte de uma infraestrutura governamental, mas a sua condição tem pouca influência no bem-estar nacional. A recuperação rápida é da maior importância. Exemplo – Infraestrutura VDI de um integrador de sistemas que fornece o ambiente de substituição de ambiente de trabalho entre outros serviços.

- **Valor elevado de serviços** - É praticamente certo que terceiros sejam afetados. O serviço é um elemento fundamental da empresa e também pode ser um elemento importante das empresas de terceiros. É possível uma influência no bem-estar nacional. Os danos à reputação são extremamente penosos e podem ser irreversíveis. A recuperação é de extrema importância; a não realização de uma recuperação com êxito no mais curto espaço de tempo possível pode ter consequências mais graves. Exemplo – infraestrutura de um sistema de videovigilância governamental.

Dado que é o cliente que melhor conhece a respetiva infraestrutura, é ele que pode tomar a melhor decisão no que se refere à solução de segurança; as diretrizes apresentadas são apenas isso – uma metodologia básica para tomar uma decisão. Mas claro que é perfeitamente possível melhorar a eficácia da sua utilização de recursos e fazer com que a sua empresa poupe algum dinheiro, mantendo a infraestrutura virtual segura. No entanto, lembre-se de que antes de implementar qualquer tipo de solução de segurança especializada, é necessário verificar e ajustar as configurações básicas de segurança da sua rede de TI. Uma rede bem administrada significa a existência de menos vetores de ataque para criminosos e menos consequências se ocorrer algum problema.

Eficiência significa integridade

A utilização eficiente de recursos é importante, mas não é nada sem um controlo eficaz. É óbvio que pode implementar uma solução Agentless para os seus back-ends de um fabricante, uma solução Light Agent para a sua VDI de outro fabricante e ainda o Controlo de aplicações de terceiros para algumas áreas críticas. Como resultado, terá três consolas de gestão, três conjuntos de políticas para configuração e manutenção e algum tráfego de atualização em excesso que tem de passar pelo seu canal de dados. Certamente que é muito mais conveniente que todas as soluções sejam provenientes de um único fabricante, com todos os indicadores e controlos bem organizados numa única consola. Todos os produtos Kaspersky Security foram concebidos para serem controlados a nível central, através do Kaspersky Security Center. Isso significa que pode gerir os seus recursos virtualizados a partir da mesma consola que utiliza para controlar a segurança dos terminais físicos.

Outra vantagem é a atualização centralizada. Não é necessário transferir o mesmo conjunto de atualizações para cada SVA em cada hipervisor; são implementadas automaticamente depois da transferência para o armazenamento KSC.

Outra característica distintiva das soluções da Kaspersky Lab é a sua disponibilidade para diferentes plataformas de virtualização. Assim, tem a liberdade de gerir um ambiente com vários hipervisores devidamente protegido e continuar a tirar partido de todos os controlos no mesmo KSC.

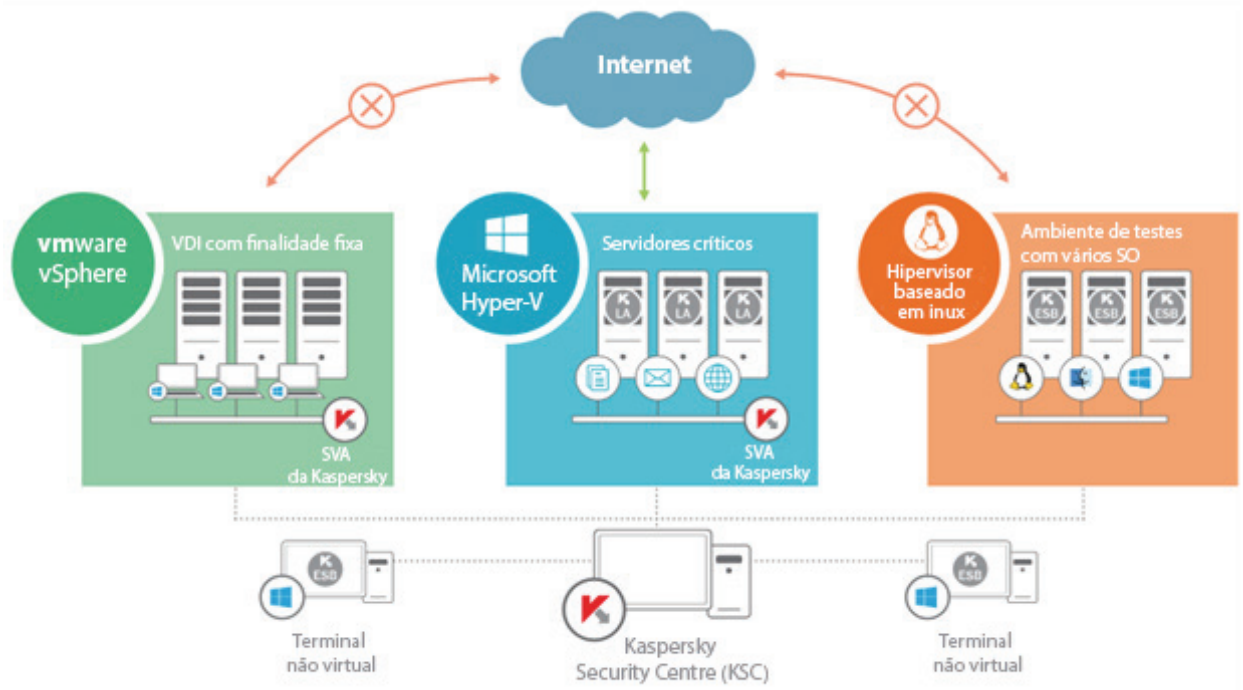

Figura 1: É possível proteger um ambiente com vários hipervisores de forma sólida e eficiente

Por exemplo, o seu núcleo Active Directory (Controladores de domínio, Sistemas de nomes de domínio, etc.) pode ser alojado nos servidores virtuais Microsoft Hyper-V, que utilizam uma VDI com base em Citrix e incluem alguns servidores de bases de dados executados no VMware ESXi. Tal como ilustrado na figura acima, também é possível gerir ambientes mistos com mais de uma plataforma de hipervisor e terminais físicos.

Neste caso, para obter o equilíbrio mais eficiente entre desempenho/segurança e atingir as taxas de consolidação ideais:

- Uma VDI isolada com uma finalidade fixa pode ser protegida pelo KSV | Agentless
- Uma infraestrutura de servidores fundamental para a empresa e que contenha dados importantes deve ser protegida pelas camadas robustas de segurança do KSV | Light Agent
- O Kaspersky Endpoint Security é a melhor proteção para um ambiente de teste com um hipervisor Linux e um conjunto de SO convidados e terminais físicos.

Em todos os casos, os produtos da Kaspersky Lab proporcionam a melhor proteção que a indústria tem para oferecer e permitem escolher entre a implementação fácil e eficiência ROI da solução KSV | Agentless, a proteção robusta do KSV | LA, ou qualquer combinação numa única estrutura de TI.

Uma vez que a Kaspersky Lab oferece aos clientes soluções de virtualização Agentless, Light Agent e Agent-based, conseguimos fazer recomendações totalmente objetivas aos nossos clientes. Não sentimos a necessidade de promover uma tecnologia específica e podemos sugerir a melhor opção ou combinação de opções para o ambiente específico de um cliente. Além disso, como as nossas soluções são baseadas no mesmo poderoso motor anti-malware e concebidas como parte de uma única plataforma de segurança integrada, sabemos que o seu sistema virtual estará seguro independentemente da solução que escolher.