LIGHT AGENT OU AGENTLESS

Guia de funcionalidades para o Kaspersky Security for Virtualization

Com a difusão da virtualização, a necessidade de soluções de segurança adequadas é evidente por si só. Embora sejam tão suscetíveis a ciberataques como qualquer sistema físico, os ambientes virtuais apresentam funcionalidades únicas que devem ser tidas em conta na altura de procurar soluções de segurança.

Apesar de proporcionarem um certo nível de proteção, as soluções padrão que não são concebidas especificamente para ambientes virtuais podem apresentar problemas, incluindo:

1) **Consumo excessivo de recursos** devido à replicação de bases de dados de assinaturas e aos motores anti-malware ativos em cada máquina virtual (VM) protegida.
2) **"Surtos"** – atualizações simultâneas da base de dados e/ou processos de verificação de anti-malware em várias máquinas virtuais, levando a um enorme aumento do consumo de recursos e causando uma perda drástica do desempenho e inclusive recusa de serviço. As tentativas de mitigar o problema ao agendar estes processos geram "janelas de vulnerabilidade", ou seja, períodos em que as verificações de malware adiadas deixam as máquinas virtuais vulneráveis a ataques.
3) **Falhas instantâneas.** As bases de dados de assinatura não podem ser atualizadas em máquinas virtuais inativas, por isso, desde o arranque da máquina até à conclusão do processo de atualização, a VM fica vulnerável ao ataque.
4) **Incompatibilidades.** Uma vez que as soluções padrão não são concebidas para lidar com funcionalidades específicas da virtualização, tais como migração de VM ou armazenamento não persistente, a sua utilização pode causar instabilidades e até bloquear o sistema.

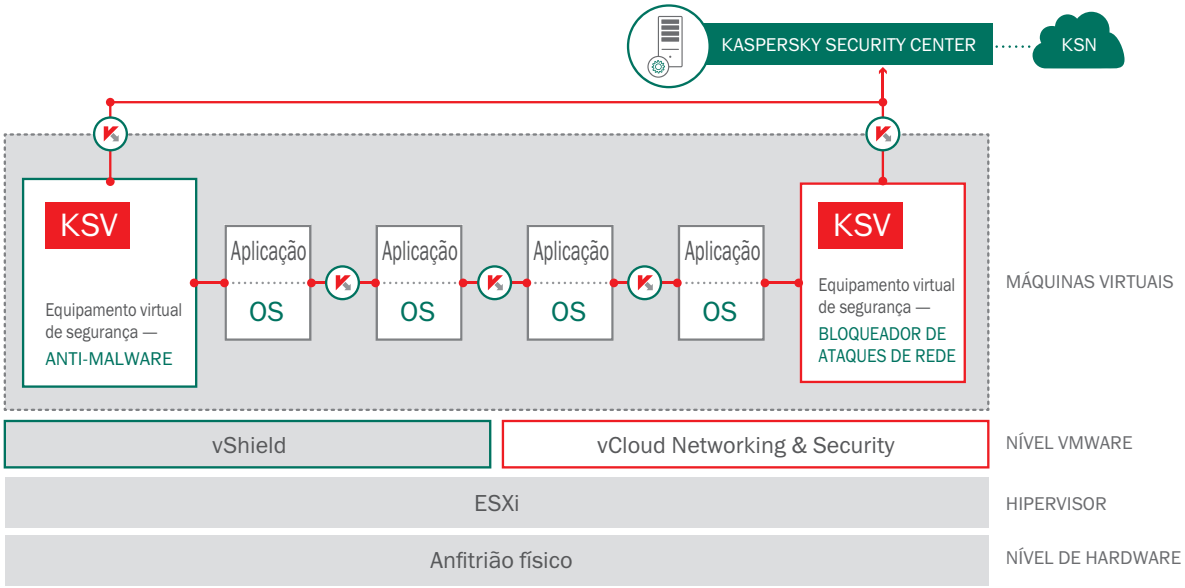
Reconhecendo a importância da segurança dos sistemas virtuais e as funcionalidades únicas que a virtualização apresenta, o VMware líder de mercado desenvolveu o vShield, uma camada defensiva específica para a sua plataforma vSphere. Esta camada cria um espaço de segurança integrado que engloba todos os ativos virtualizados e permite um acesso fácil e eficiente através de soluções de segurança adequadas. Uma vantagem óbvia desta abordagem é que a proteção "Agentless" dos terminais virtualizados passa a ser uma opção. Apenas é necessário um equipamento virtual de segurança (SVA), ou seja, uma máquina virtual especializada que possui um motor de verificação anti-malware e uma base de dados de assinatura, removendo esta carga das máquinas virtuais individuais e reduzindo bastante o consumo de recursos. As soluções de segurança compatíveis com vShield, capazes de aproveitar todas as funcionalidades que o ambiente VMware oferece, podem trazer várias vantagens aos utilizadores através desta abordagem.

KASPERSKY SECURITY FOR VIRTUALIZATION | AGENTLESS

O Kaspersky Security for Virtualization | Agentless foi especificamente concebido para tirar partido de todas as vantagens do vShield. O equipamento virtual de segurança (SVA), pronto para implementação imediata, conta com o premiado motor anti-malware da Kaspersky Lab e, como tal, beneficia de taxas de deteção superiores. O apoio ao serviço Kaspersky Security Network, assistido pela nuvem, garante o tempo de reação mais rápido e, mais importante ainda, reduz significativamente o número de falsos positivos. Pode ser utilizado um segundo SVA para fornecer a tecnologia de bloqueio de ataques de rede da Kaspersky, em conjunto com o componente VMware vCloud Networking and Security.

No entanto, existem lacunas na abordagem "Agentless".

Para começar, o VMware é o único fabricante que dispõe de uma camada de segurança intermédia; no caso das outras plataformas, a solução de segurança tem de encontrar outra forma para aceder às VM individuais. Em segundo lugar, o vShield não dá acesso aos processos internos das máquinas virtuais, diminuindo significativamente a capacidade de qualquer solução proporcionar uma maior proteção contra malware avançado a este nível.



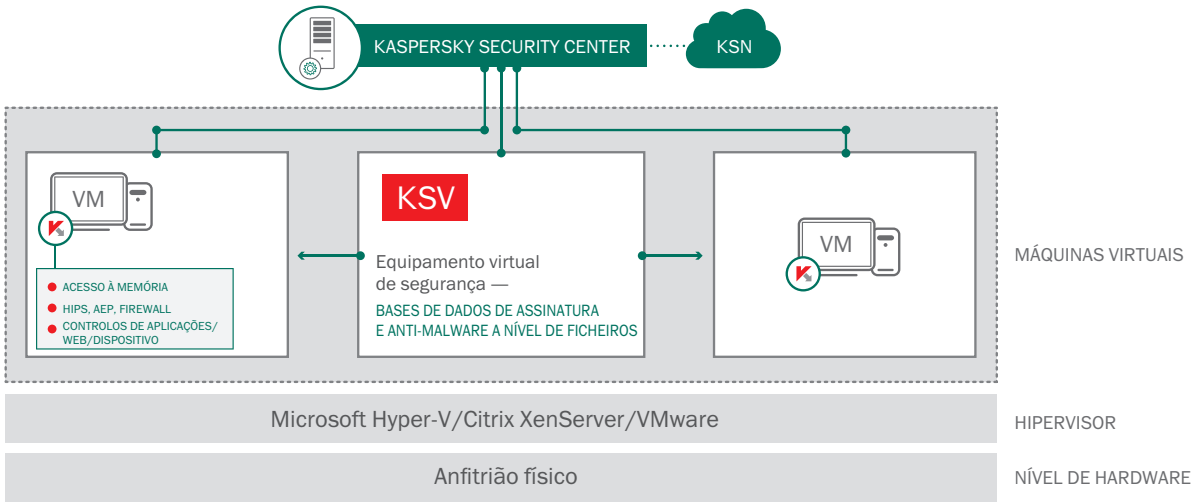
Foi introduzida outra abordagem para superar estas limitações e implementada uma aplicação pequena e leve para a VM que está a ser protegida, além do SVA. Esta aplicação é conhecida como "Light Agent". O motor de verificação de ficheiros e as bases de dados são geridos de forma centralizada e esta aplicação tem um impacto mais reduzido na memória da VM do que uma solução Full Agent, fornecendo acesso ao sistema de ficheiros da VM, à memória e aos processos internos. Como resultado, podem ser implementadas técnicas de segurança adicionais mais avançadas.

KASPERSKY SECURITY FOR VIRTUALIZATION | LIGHT AGENT

O **Kaspersky Security for Virtualization** | **Light Agent** foi criado para as três plataformas de virtualização mais populares: Citrix, Microsoft Hyper-V e VMware. O verificador anti-malware e as bases de dados de assinatura encontram-se num SVA dedicado, tal como acontece na tecnologia Agentless, libertando assim recursos para a implementação de VM adicionais para que as taxas de consolidação sejam otimizadas. Além disso, com um Light Agent em execução em cada SO convidado, torna-se possível implementar a maior parte das tecnologias avançadas disponíveis para máquinas físicas através do **Kaspersky Endpoint Security for Business**. É possível implementar um conjunto completo de controlos de terminais, como HIPS (Sistema de prevenção de invasão com base em anfitrião), uma firewall do proprietário e um conjunto de ferramentas de Gestão de sistemas. É criado um poderoso perímetro defensivo multicamadas, capaz de lidar com os tipos de malware mais sofisticados e com ameaças de dia zero.

Embora garanta um nível de proteção mais elevado, a solução **Light Agent** pode parecer "mais pesada" do que o seu equivalente **Agentless** e requer um pouco mais de atenção na altura de implementar novas VM. Mas, mesmo estas questões não são tão simples como parecem.

Para uma melhor compreensão, é preciso analisar aprofundadamente a funcionalidade das soluções **Agentless** e **Light Agent** e as ameaças que devem combater.



AMEAÇAS VS. FUNCIONALIDADES

As máquinas virtuais são tão vulneráveis como os seus equivalentes físicos e porventura ainda mais: nas redes virtualizadas ultrarrápidas, a propagação da infeção pode ser devastadora. Por isso, é importante identificar as falhas na segurança da sua infraestrutura virtual e implementar medidas adequadas em proporção às potenciais ameaças. Abaixo, examinamos as potenciais ameaças aos sistemas virtuais e as tecnologias utilizadas para as combater.

MALWARES EXECUTÁVEIS

O anti-malware é essencial para lidar com ameaças básicas como anexos traiçoeiros recebidos por e-mail, leisureware infetado ou malware temporário executável. O motor de combate a malware é a tecnologia central das configurações **Agentless** e **Light Agent** do **Kaspersky Security for Virtualization,** apesar de este aceder aos sistemas de ficheiros da VM protegida através de diferentes meios consoante o caso.

Outra forma de evitar que os agentes de malware danifiquem os seus ativos virtualizados é através do Controlo de aplicações com listas brancas dinâmicas. O malware é travado quando apenas o software legítimo e seguro estiver autorizado a ser executado. O Kaspersky Security for Virtualization | Light Agent permite que o Controlo de aplicações seja ativado em VM, apesar de o Kaspersky Security for Virtualization | Agentless, que funciona através do vShield, não ser capaz de suportar os controlos de terminais.

MALWARE SEM CORPO

Existe malware sofisticado que não tem "corpo", o que significa que não é possível encontrar nada no sistema de ficheiros. Gerado por um ficheiro executável previamente lançado ou injetado através de um exploit, este tipo de malware não pode ser detetado pelas medidas anti-malware tradicionais. São necessárias medidas de prevenção avançadas anti-malware, capazes de manter sob vigilância processos na memória e de bloquear imediatamente programas envolvidos em atividades perigosas, quer sejam suspeitas ou evidentes. O **Kaspersky Security for Virtualization | Light Agent** está munido de uma gama de tecnologias capazes de bloquear invasões à memória da VM. Estas incluem:

- O Observador do sistema, que monitoriza o comportamento do programa, analisando eventos do sistema. Tal é suportado por:
- BSS – Assinaturas de transmissão de comportamento, que identificam padrões de comportamento característicos da atividade de malware.
- Controlo de privilégios, que impede a aplicação de efetuar alterações não solicitadas, incluindo injeção do processo.

Estas ferramentas permitem que o Sistema de prevenção de invasão com base em anfitrião (HIPS) localize e pare processos não autorizados na memória da VM.

O **Kaspersky Security for Virtualization | Agentless** só consegue detetar alterações ao nível do sistema de ficheiros, devido às limitações da API vShield.

EXPLOITS

A exploração de vulnerabilidades encontradas nos componentes dos sistemas e nas aplicações populares continua a ser um dos mecanismos de ataque mais eficazes. Embora seja possível impedir estas invasões utilizando as tecnologias acima mencionadas, o programa afetado pode funcionar a um nível de privilégios elevado, limitando o controlo das suas atividades.

O método mais eficaz de combate a esta ameaça é evitar que os exploits façam aquilo que o seu nome indica, ou seja, explorar as vulnerabilidades. Tal é possível através do reconhecimento da sequência de ações caraterísticas dos exploits, à medida que ocorrem; conforme realizado pela Prevenção automática de exploit (AEP) da Kaspersky. A eficiência desta tecnologia ficou comprovada através de uma série de testes independentes realizados pelo instituto MRG Effitas. Estes testes demonstraram que, mesmo com todos os outros componentes de proteção desligados, a tecnologia AEP da Kaspersky continuava a ser 100% eficaz contra ataques que utilizavam exploits. Mesmo os exploits desconhecidos de dia zero são bloqueados por esta tecnologia pró-ativa.

O **Kaspersky Security for Virtualization | Light Agent** está equipado com esta funcionalidade avançada, o que o torna particularmente útil em infraestruturas de computadores pessoais virtuais (VDI) implementadas para substituir computadores pessoais físicos, com os seus riscos de infeções "drive-by" proporcionalmente mais elevados.

O **Kaspersky Security for Virtualization | Agentless** depende das capacidades do vShield, que não tem funcionalidades semelhantes à tecnologia AEP da Kaspersky.

ROOTKITS

O malware sofisticado é muitas vezes capaz de se esconder, com a ajuda dos chamados "bootkits" e "rootkits", impedindo a deteção através do anti-malware tradicional. Estas ferramentas insidiosas tentam carregar malware o mais cedo possível, de modo a que permaneça oculto enquanto ganha privilégios elevados dentro do sistema. A tecnologia Anti-Rootkit da Kaspersky é capaz de detetar e erradicar mesmo o malware com este nível de ocultação. Funciona ao nível da memória e do sistema de ficheiros e, para isso, requer o acesso à memória RAM e aos processos da máquina convidada.

O **Kaspersky Security for Virtualization | Light Agent** pode oferecer esta tecnologia uma vez que tem total acesso aos recursos da máquina convidada.

O **Kaspersky Security for Virtualization | Agentless** só consegue aceder ao sistema de ficheiros, não possuindo todas as capacidades Anti-Rootkit.

ATAQUES À REDE

Há ameaças que se aproveitam das funcionalidades do sistema de rede, permitindo que o autor do ataque consiga informações cruciais sobre a rede que está a ser atacada, tenha acesso aos recursos pretendidos do sistema ou interfira com o seu bom funcionamento. Estas ameaças incluem a verificação de portas, os ataques de negação de serviço, os ataques de esvaziamento da memória intermédia e outras ações maliciosas. Estes ataques exigem medidas de prevenção especializadas como as fornecidas pelo Bloqueador de ataques de rede da Kaspersky. Tal como o nome sugere, esta tecnologia impede ataques à rede, com a ajuda de um IDS (Sistema de deteção de invasão) e utilizando algoritmos heurísticos para identificar até os padrões de ataque mais complexos.

O **Kaspersky Security for Virtualization | Agentless** e o **Kaspersky Security for Virtualization | Light Agent** incluem estas tecnologias de rede.

WEBSITES MALICIOSOS

Uma das fontes mais comuns de infeção é um website malicioso ou infetado. Embora raramente afete servidores virtualizados, pode constituir uma séria ameaça à VDI de substituição de ambiente de trabalho se os utilizadores tiverem acesso à Internet sem restrições. É aqui que as tecnologias Web da Kaspersky entram em ação. O anti-phishing impede que os utilizadores acedam a websites denunciados como perigosos, utilizando informações obtidas através do **Kaspersky Security Network** e constantemente atualizadas, com a ajuda de milhões de voluntários do KSN em todo o mundo. De momento, os websites de phishing ocultos também estão bloqueados, graças a um motor heurístico que analisa o texto de origem da página carregada, detetando sinais de códigos maliciosos. A tecnologia de **Controlo Web** tem a vantagem adicional de restringir o acesso a websites que não estão relacionados com o trabalho, como jogos ou redes sociais, impedindo os utilizadores de desperdiçarem tempo precioso em atividades não relacionadas com o trabalho.

O **Kaspersky Security for Virtualization** | **Agentless** não inclui estas funcionalidades com base em anfitrião, mas o **Kaspersky Security for Virtualization** | **Light Agent** inclui, tornando-o mais adequado para VDI com acesso à Internet.

ATAQUES COM BASE EM PERIFÉRICOS

Tradicionalmente, um dos métodos mais eficazes para introduzir uma infeção numa rede de TI é através de armazenamento externo. Apesar de as infeções de rede parecerem agora uma grande ameaça em termos de números, o armazenamento externo continua a ser um perigo considerável, especialmente quando faz parte de um ataque cuidadosamente planeado e direcionado. Vale a pena mencionar que os periféricos não utilizados para armazenamento sem controlo também podem representar uma ameaça; os casos conhecidos incluem, por exemplo, firmware infetado de impressoras. As unidades de armazenamento externo continuam a ser um dos principais métodos de transporte de dados confidenciais.

Apesar de, geralmente, não ser fácil para uma pessoa não autorizada ter acesso às máquinas físicas que hospedam a infraestrutura virtual, tal é possível e existem ainda casos de empresas onde essa possibilidade é considerada um risco demasiado elevado. Em relação a VDI de substituição de ambiente de trabalho, mesmo os clientes magros mais simples podem ter portas USB.

Como tal, o controlo de periféricos torna-se uma precaução sensata , facilmente alcançada através da tecnologia **Controlo de dispositivos da Kaspersky** . Permite a prevenção ou restrição da utilização de dispositivos e de tipos de bus específicos. Além disso, como é óbvio, é possível configurar exceções, de modo a que os periféricos indispensáveis para o trabalho possam continuar ser utilizados.

Tal como acontece no caso de outras tecnologias de controlo, o Controlo de dispositivos faz parte do **Kaspersky Security for Virtualization** | **Light Agent**, mas não do **Kaspersky Security for Virtualization** | **Agentless.**

FUGA DE DADOS

A fuga de dados empresariais de uma rede de TI pode provocar muitos danos a uma empresa, incluindo danos à sua reputação que podem ter consequências duradouras e prejudiciais. Desta forma, pode ser necessário restringir o número de meios através dos quais as informações são partilhadas. O **Controlo de aplicações da Kaspersky** e o **Controlo de dispositivos** são úteis neste caso. O Controlo de aplicações pode evitar a execução de aplicações perigosas, tais como mensagens instantâneas ou hospedagem de ficheiros e aplicações de cliente P2P, e o controlo de dispositivos restringe a utilização do armazenamento externo, que pode ser usado para a apropriação de dados confidenciais.

Como acima referido, estas duas tecnologias estão incluídas no **Kaspersky Security for Virtualization** | **Light Agent**, mas não estão incluídas no **Kaspersky Security for Virtualization** | **Agentless**.

AGENTLESS VS LIGHT AGENT: QUAL A MELHOR SOLUÇÃO?

A resposta pode parecer clara para alguns leitores: o **Kaspersky Security for Virtualization** | **Light Agent** está repleto de funcionalidades avançadas que não estão incluídas no **Kaspersky Security for Virtualization** | **Agentless**, por isso a solução Light Agent é obviamente melhor. Mas não tire conclusões precipitadas, é um pouco mais complicado do que parece.

Em primeiro lugar, há a questão da proteção instantânea disponibilizada pelo **Kaspersky Security for Virtualization** | **Agentless**. As máquinas virtuais ficam protegidas desde o momento do arranque, o que pode ser importante se já tiver uma infeção na sua rede virtualizada (e se não for possível criar a sua VM a partir de uma imagem que contenha a aplicação **Light Agent**).

Em alguns casos, o **Kaspersky Security for Virtualization** | **Light Agent** pode ficar aquém do **Kaspersky Security for Virtualization** | **Agentless** em termos de desempenho. Para escolher a melhor opção de segurança para a sua instalação virtual e tirar o máximo proveito do projeto de virtualização, tem de ponderar cuidadosamente as potenciais ameaças, o valor dos dados que estão a ser protegidos e as diferentes camadas de proteção necessárias.*

Tenha em atenção que qualquer combinação da proteção Agentless para VMware e de segurança baseada no Light Agent, para qualquer uma das três plataformas, ou para todas elas, é abrangida por uma única licença **Kaspersky Security for Virtualization**. Mesmo que esteja a implementar um sistema Citrix, VMware ou Microsoft, todos são controlados através da interface intuitiva de "janela única" do **Kaspersky Security Center**.

* Consulte o documento técnico "Kaspersky Security for Virtualization: compreender a diferença" para obter mais informações sobre como escolher a melhor combinação de soluções Kaspersky para proteger a sua infraestrutura virtual.

KASPERSKY lab