SEGURANÇA PARA MÁQUINAS VIRTUAIS

Conheça a solução da Kaspersky Lab

CICLOS ADICIONAIS, MAIS CUSTOS

Para qualquer provedor de serviços, é essencial considerar a redução do impacto sobre o desempenho ao escolher os componentes de software de sua oferta de infraestrutura como serviço. Os ciclos adicionais exigidos pelos componentes de software diminuem a taxa de consolidação geral, levando a custos adicionais com hardware e as caras licenças de plataformas que seguem.

O software de segurança implementado nas infraestruturas virtualizadas é um dos exemplos mais notáveis de impacto negativo sobre o desempenho. Porém, poucos sabem que isso acontece por causa de um erro simples e muito comum: a utilização da segurança de endpoints tradicional com base em agentes em um ambiente virtual.

As soluções convencionais de segurança de endpoints foram criadas para proteger computadores físicsos que quase sempre têm mais recursos que o necessário para sua carga de trabalho e executam um único sistema operacional, que não precisa disputar ou compartilhar esses recursos com outros sistemas operacionais. Quando vários sistemas operacionais precisam coexistir, a escolha de uma arquitetura de segurança inadequada pode gerar inconvenientes, como nestes três cenários comuns:

- **Tempestades de atualizações:** quando vários agentes de endpoints tentam atualizar os bancos de dados de definições de malware ao mesmo tempo
- **Tempestades de verificações de malware:** quando vários agentes de endpoints tentam executar verificações de malware ao mesmo tempo
- **Surto de vírus:** quando um servidor de controle de segurança fortalece a segurança ao detectar um ataque em um nó ou uma rede. Essa medida de segurança produz um pico imediato de consumo de recursos por todos os agentes de segurança.

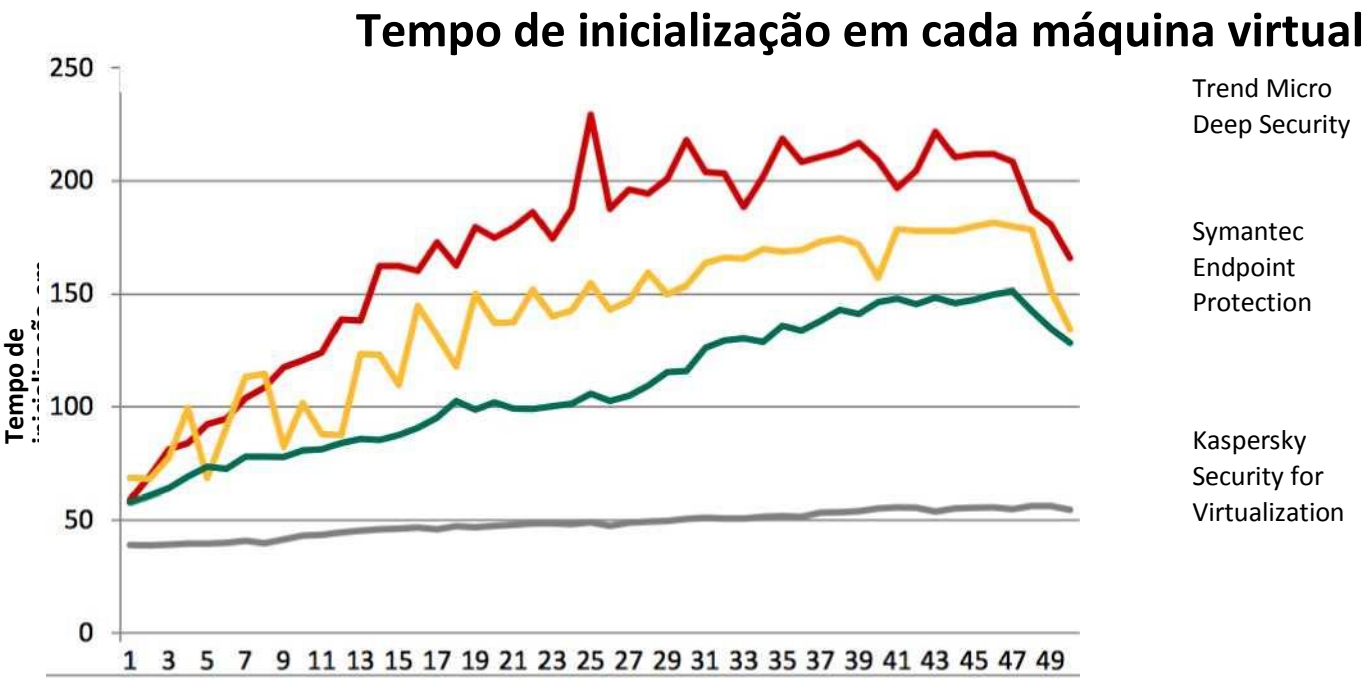
Qualquer desses três cenário pode tornar a infraestrutura mais lenta, fazer o sistema e ou servidor deixarem de responder e até causar uma interrupção total das operações. Mesmo com os agentes de segurança de endpoints atuais, compatíveis com a virtualização e que aplicam técnicas como a aleatorização do horário das atualizações ou verificações para reduzir seu impacto, a "taxa de segurança" ainda é muito grande. A segurança pode se tornar um peso para seus clientes.

Você já recebeu alguma ligação de um cliente irritado dizendo: <bi>"A verificação antivírus que vocês executaram ontem à noite afetou nosso

ENTENDENDO A DIFERENÇA: USANDO UMA SEGURANÇA

Menor impacto sobre o desempenho

O desempenho é o fator mais importante nos ambientes virtualizados. Tamos aqui um exemplo de como o impacto sobre o desempenho pode ser grave quando a solução de segurança escolhida não é a ideal.[1]



O Kaspersky Security for Virtualization oferece excelente proteção granular em vários níveis para ambientes de VDI e servidores virtuais com impacto mínimo sobre a reação de suas cargas de trabalho virtualizadas. Para conseguir isso, todas as tarefas que consomem muitos recursos são descarregadas dos endpoints para uma máquina virtual especial, chamada de Dispositivo Virtual de Segurança (SVA, Security Virtual Appliance). O SVA mantém um único banco de dados sempre atualizado de definições de malware, gerencia as operações de leitura/gravação do armazenamento de modo flexível e realiza a alocação e o balanceamento de recursos. Ao mesmo tempo, agentes com 'pouca exigência de recursos' em cada máquina – os agentes leves – mantêm a proteção avançada, verificando processos maliciosos na RAM virtual, fornecendo a funcionalidade de IPS/IDS, impondo políticas de segurança, como controles da Web,

[1] Fonte: Virtual Desktops Security Test Report, AV-TEST, maio de 2014

IMPLEMENTAÇÃO DO CONTROLE DE APLICATIVOS BASEADO EM REFERÊNCIAS E DA NEGAÇÃO PADRÃO

O Kaspersky Security for Virtualization ativa a funcionalidade de controle de aplicativos nas máquinas virtuais protegidas. Considerando a realidade de que muitos arquivos se repetem em todos os desktops (por exemplo, arquivos do Microsoft Windows), isso evita o desperdício de recursos valiosos ao verificar arquivos que estão limpos. Além disso, o modo de Negação Padrão garante que apenas os aplicativos implementados no sistema de referência têm permissão para ser executados. Em associação com tecnologias inteligentes, como o cache compartilhado, isso facilita o desempenho máximo dos desktops e servidores protegidos.

PROVISIONAMENTO RÁPIDO

O Kaspersky Security for Virtualization | Light Agent dá suporte à clonagem vinculada e total. Assim, para providenciar uma nova máquina virtual, basta simplesmente clonar um modelo com o KSV | Light Agent pré-instalado. Ao concluir a clonagem, a nova máquina será protegida automaticamente pelo SVA que reside no mesmo host.

CONTROLE BASEADO EM FUNÇÕES TRANSPARENTE E CONVENIENTE

Toda a funcionalidade do Kaspersky Security for Virtualization é gerenciada em um único console (Kaspersky Security Center), no qual também são gerenciadas as soluções de segurança de endpoints da Kaspersky Lab. A existência de uma exibição única para gerenciar a segurança de endpoints. físicos, virtuais e móveis torna mais fácil eliminar falhas de segurança criadas quando são usados vários consoles diferentes para ajustar funcionalidades de segurança diferentes.

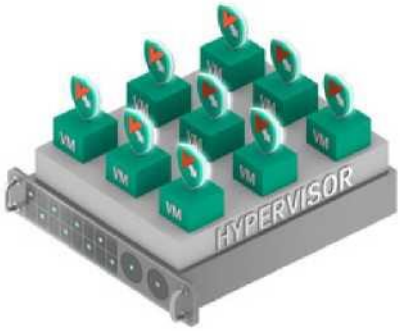
Os controles de acesso baseado em funções do Kaspersky Security Center proporcionam uma conveniência adicional: funções de gerenciamento diferenciadas para os vários especialistas, tanto na organização do provedor de serviços quanto na do cliente.

RELATÓRIOS DE STATUS DE SEGURANÇA FLEXÍVEIS

Os elaborados relatórios personalizáveis podem ser integrados com os relatórios gerais de TI, proporcionando uma visualização simples do status de segurança de toda a infraestrutura.

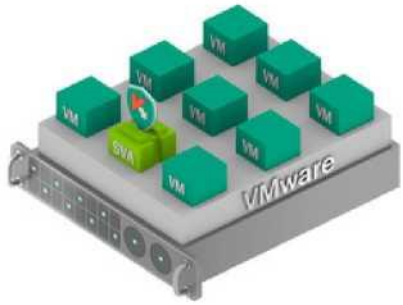
INDEPENDÊNCIA DO HIPERVISOR: OS CLIENTES PODEM ESCOLHER SUA PLATAFORMA

O Kaspersky Security for Virtualization | Light Agent dá suporte às plataformas de virtualização VMware, Microsoft e Citrix, além de suporte total ao VMware Horizon View e ao Citrix XenDesktop.



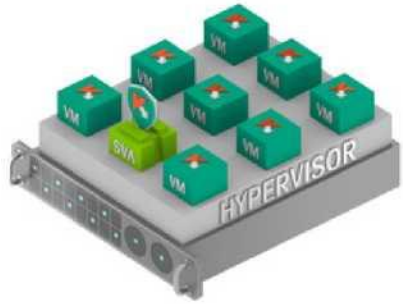
Com base em agentes

Utilizacão não eficiente



Sem agentes

Eficiente, mas faltam recursos avançados de segurança



Agente leve

Combina eficiência com recursos avançados de segurança por meio de um agente de segurança leve e um dispositivo virtual de segurança

Na plataforma VMware, o Kaspersky Security for Virtualization também pode funcionar no modo Sem agentes.
Para saber mais, consulte a arquitetura VMware de referência para 1.000 VDs protegidos pelo KSV |

Do guia de arquitetura de referência:

"Todos os 1.000 usuários que executam uma carga de trabalho normal de escritório concluíram com êxito o pool de testes sem travas nas CPUs, sem esgotar a memória ou sobrecarregar os sistemas de

A MELHOR PROTEÇÃO ABSOLUTA

É importante entender que, no cenário Sem agentes, o número de informações e tecnologias disponíveis para qualquer solução de segurança é limitado pela API do vShield, o que torna fundamental a qualidade da detecção de assinaturas, do mecanismo heurístico e do sistema de classificação com base na nuvem. A Kaspersky Lab oferece a melhor proteção do setor, como mostra o resumo das pontuações de 2014 em testes independentes de produtos corporativos, para o consumidor e para dispositivos móveis:

Pensou nisso? Em um ambiente onde os pesquisadores da Kaspersky Lab descobrem 325.000 itens exclusivos de malware *a cada dia*, até uma diferença de 1% nas taxas de detecção pode fazer a diferença entre o bloqueio bem-sucedido de um ataque e o início de um processo de investigação e neutralização

HOSPEDANDO IMPLEMENTAÇÕES SEGURAS NA NUVEM

Baixo impacto sobre o desempenho, provisionamento mais rápido, controles transparentes e flexíveis, e relatórios flexíveis podem ser ótimos argumentos de venda para sua solução. Mas, o melhor é a maior segurança. Sua capacidade de usar KPIs para medir o desempenho em vários serviços ajudará a garantir que todos os serviços sejam fornecidos exatamente de acordo com os requisitos e que todos os desvios sejam controlados integralmente.

A Open Data Center Alliance recomenda usar KPIs para medir o desempenho e facilitar as taxas de detecção por meio do rastreamento de desvios. Pensou nisso? O tempo médio de ocupação de uma violação de dados de grande porte é de **meses** – 98 dias nas organizações de serviços financeiros, chegando a 197 dias no varejo.[2] Quantos de seus clientes realmente desejam dar aos criminosos virtuais a possibilidade de dominar livremente suas redes, peneirando dados sigilosos e descobrindo lentamente os detalhes de sua infraestrutura, especialmente para lançar ataques futuros?

Porém, 44% das organizações não mede o 'Tempo médio de identificação' (MTTI, Mean Time to Identify, também chamado de 'tempo de ocupação'). Como você sabe que está reduzindo o tempo de ocupação, se não mede? Como é possível melhorar a resposta a incidentes, se você não sabe o que está detectando? O Kaspersky Security for Virtualization | Light Agent proporciona as melhores taxas de detecção do setor, sendo capaz de reduzir drasticamente o tempo de ocupação e impulsionar o desempenho. Assim, seus clientes têm a oportunidade de melhorar os KPIs em toda a infraestrutura, tornando a segurança um benefício importante de sua proposta de provisão de serviços.

A SEGURANÇA ESPECÍFICA PARA VIRTUALIZAÇÃO PROPORCIONA BENEFÍCIOS PARA OS NEGÓCIOS

A segurança de TI padrão não é adequada para ambientes virtuais. E se o software de segurança que você oferece a seus clientes pudesse realmente impulsionar a virtualização – com todas as vantagens envolvidas – em vez de limitá-la? Dos processos de negócios à funcionalidade de aplicativos críticos e dados altamente sigilosos, o valor da virtualização vai muito além de sua atratividade original como uma ferramenta flexível para utilizar recursos de maneira eficiente. Esses mesmos benefícios da tecnologia agora também são benefícios para os negócios; como provedor de serviços, além de proteger a tecnologia, você também protege os benefícios empresariais que a acompanham.

43% dos profissionais de TI acreditam que a segurança representa uma barreira

46% dos profissionais de TI acreditam que podem proteger a infraestrutura virtual usando os softwares de segurança

Ponemon Institute: Cyber Security Incident Response - Are We As Prepared As We Think? Janeiro de 2014 [3] Relatório de Riscos Globais de TI de 2014 da Kaspersky Lab

SOBRE A KASPERSKY LAB

A Kaspersky Lab é a maior empresa de capital fechado e uma das empresas no segmento de segurança de computadores que mais cresce no mundo. A empresa está classificada entre os quatro principais fornecedores de soluções de segurança para usuários de endpoints do mundo (IDC, 2014). Desde 1997, a Kaspersky Lab inova na área de segurança cibernética e oferece soluções de segurança digital e informações estratégicas eficientes para grandes corporações, empresas de pequeno e médio porte e para o consumidor final. A Kaspersky Lab é uma empresa internacional que opera em quase 200 países e territórios no mundo

PARTICIPE DA CONVERSA

Assista-nos no

Curta-nos no Facebook

Examine o nosso

Siga-nos no Twitter

Junte-se a nós no

Saiba mais em usa.kaspersky.com/business-security/virtualization

AO Kaspersky Lab
500 Unicorn Park, 3rd Floor Woburn, MA 01801 EUA
Fone: 866-563-3099 | E-mail: corporatesales@kaspersky.com
Para saber mais, visite: usa.kaspersky.com

KASPERSKY lab O PODER DA PROTEÇÃO