KASPERSKY SECURITY FOR VIRTUALIZATION E VMWARE NSX

PROTEÇÃO SUPERIOR PARA CENTRAIS DE DADOS BASEADAS NO SOFTWARE

Os dados são o patrimônio mais importante de sua empresa. Por isso, a forma e o lugar onde esses dados são armazenados, processados e transmitidos são fundamentais não apenas para conseguir uma vantagem competitiva maior, mas também para melhorar a eficiência operacional e garantir a continuidade dos negócios.

Existem no mercado muitas soluções excepcionais de processamento, armazenamento e integração de dados. Porém, as soluções de rede podem ser especialmente complexas, inflexíveis e, frequentemente, estão vinculadas e limitadas pela plataforma de hardware subjacente. Isso, por sua vez, obstrui a agilidade de sua central de dados e sua capacidade de atender rapidamente às mudanças nos requisitos dos negócios.

A VMware® e a Kaspersky Lab resolvem essas questões juntas, por meio de uma solução conjunta desenvolvida sobre uma central de dados baseada no software extremamente eficiente, equipada com funcionalidades avançadas de segurança para garantir excelente proteção contra ameaças internas e externas.

SERVIÇOS INTEGRADOS DO VMWARE NSX

- Firewall distribuído
- Monitoramento de atividades do servidor
- Redes virtuais (VXLAN)
- VPN (IPSec, SSL L2VPN)

KASPERSKY SECURITY FOR VIRTUALIZATION

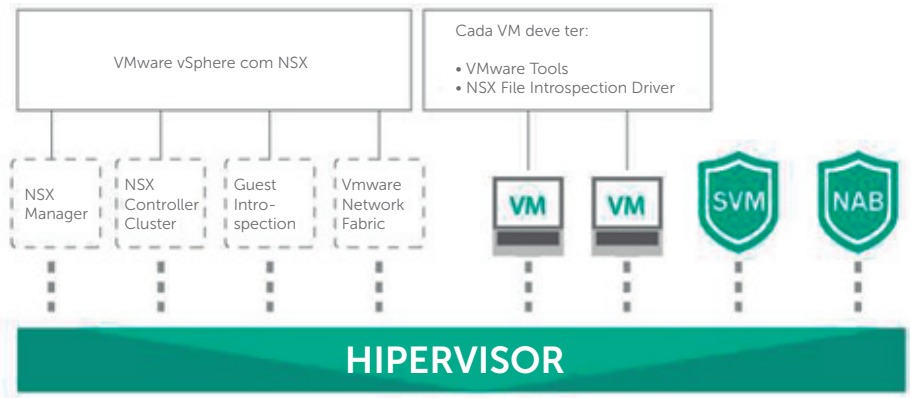
- Antimalware
- Automação da segurança
- Integração com marcas de segurança
- IDS/IPS de rede virtual
- Integração baseada em políticas
- Verificação de toda a infraestrutura, até de VMs desligadas

O Kaspersky Security for Virtualization Agentless foi criado especificamente para proteger centrais de dados baseadas no software desenvolvidas com tecnologias VMware vSphere com NSX. Nossa solução de segurança proporciona funcionalidades avançadas quase sem impacto sobre a eficiência da plataforma. Assim, você tira proveito de uma solução antimalware líder do setor e mantém altas taxas de consolidação.

COMO FUNCIONA A INTEGRAÇÃO DA PLATAFORMA

O VMware NSX® reproduz a rede de sua central de dados usando um modelo baseado no software. Assim, você pode trabalhar com diversos pools de recursos de rede, criando ou reconfigurando dinamicamente toda a topologia da rede em questão de segundos, usando uma abordagem de segurança de "confiança zero".

A forte integração entre a plataforma VMware NSX e o Kaspersky Security for Virtualization proporciona proteção automatizada para todas as máquinas virtuais (VMs) e a rede virtualizada contra as ameaças mais avançadas. Não é necessário instalar um agente de segurança nas VMs; a proteção contínua e superabrangente é fornecida sem afetar os recursos de sua plataforma virtualizada.



MÁQUINA VIRTUAL DE SEGURANÇA

- Integração nativa com o VMware NSX
- Compatível com o NSX e o vShield Endpoint

BLOQUEADOR DE ATAQUES DE REDE

- Proteção eficiente de redes
- Controle do tráfego da Web com a verificação de URLs
- Analisador heurístico para proteger aplicativos
- Proteção imediata de toda a infraestrutura

A interação nativa entre a plataforma de virtualização e a solução de segurança permite que a central de dados baseada no software responda em tempo real a qualquer incidente de segurança na infraestrutura.

PROJETADO ESPECIFICAMENTE PARA A SEGURANÇA DO VMWARE NSX

- O mecanismo antimalware mais premiado do setor reconhece e bloqueia ameaças virtuais conhecidas, desconhecidas e até de dia zero.
- A implementação automatizada para VMware NSX permite que a máquina virtual de segurança (SVM, Security Virtual Machine) seja exibida automaticamente no hipervisor, de acordo com os requisitos das VMs protegidas localizadas nesse host.
- Com a integração das políticas de segurança, cada VM recebe funcionalidades de segurança precisas, definidas pelas políticas corporativas de acordo com a função individual da VM.
- A integração com as marcas de segurança do NSX permite que a central de dados baseada no software responda aos incidentes de segurança em tempo real, reconfigurando automaticamente toda a infraestrutura virtual, se necessário.
- A defesa proativa contra ameaças avançadas é fornecida pela Kaspersky Security Network baseada em nuvem.
- O suporte simultâneo para o NSX e o vShield Endpoint garante que suas estratégias de TI e de segurança estejam totalmente alinhadas com as suas necessidades de negócios.

KASPERSKY lab

SEGURANÇA E MONITORAMENTO AUTOMATIZADOS

• A verificação de toda a infraestrutura protege todas as VMs, on-line e off-line, para melhorar ainda mais a cobertura de segurança em toda a infraestrutura.
• A verificação rotineira de todas as VMs pode ser pré-programada em nível granular. Assim, é possível coordenar as tarefas de segurança de acordo com as suas necessidades.
• A autoproteção e o monitoramento avançado baseado em SNMP garantem o funcionamento contínuo das SVMs, capazes de fornecer informações sistemáticas para ferramentas de monitoramento de terceiros e melhorando o controle.
• A proteção avançada nunca será interrompida, mesmo que a carga de trabalho seja transferida de um host para outro. As funcionalidades do VMware vMotion e de recuperação de desastres têm suporte integral.
• A integração nativa com o servidor VMware vCenter e com o NSX Manager permitem que sua camada de segurança esteja sempre ciente de todas as alterações na infraestrutura.

O MELHOR EQUILÍBRIO ENTRE PROTEÇÃO E DESEMPENHO

• A premiada proteção antimalware projetada para virtualização permite que as tarefas de verificação de arquivos sejam descarregadas da VM individual em uma SVM dedicada de modo a melhorar a eficiência.
• O sistema de detecção e prevenção de invasões (IDS/IPS) da rede virtual funciona no modo sem agentes, blindando toda a infraestrutura virtualizada contra ameaças baseadas na rede.
• A otimização em cache garante que os arquivos verificados recentemente não passem novamente pela verificação de rotina.
• A eficiência no uso de recursos de nossa solução de segurança melhora o desempenho da TI e reduz a carga sobre a infraestrutura de computação.

CONFIABILIDADE E GERENCIABILIDADE EXCEPCIONAIS

• Com um console de gerenciamento unificado para dispositivos virtuais, físicos e móveis, você pode impor políticas de segurança consistentes para todas as propriedades de TI.
• Implementação sem inatividade; não é necessário reiniciar as VMs, nem colocar o servidor host em modo de manutenção.
• A coordenação inteligente de tarefas de verificação e a automação eliminam os picos de consumo de recursos do hipervisor de modo a preservar a eficiência geral da plataforma.
• Os relatórios e o monitoramento repletos de recursos facilitam o gerenciamento e a supervisão da segurança em toda a organização.

O resultado é um ambiente virtualizado corporativo flexível que proporciona excelente eficiência de desempenho e a melhor segurança do setor.

KASPERSKY lab

SEGURANÇA IDEAL PARA SUA CENTRAL DE DADOS BASEADA NO SOFTWARE

As infraestruturas virtuais e físicas enfrentam as mesmas ameaças de segurança: os criminosos virtuais não fazem distinções. Você não pode se arriscar a comprometer a sua segurança. Nem o seu desempenho.

1 AS AMEAÇAS VIRTUAIS ESTÃO SE TORNANDO COISA DO PASSADO

Baseado no mecanismo de segurança mais premiado do setor, o Kaspersky Security for Virtualization ajuda a combater as vulnerabilidades e ameaças mais avançadas em todo o seu cenário de TI virtualizada. Nossa solução de segurança foi projetada especificamente para explorar as vantagens tecnológicas que as plataformas de virtualização oferecem, proporcionando segurança eficiente com velocidade ideal e eficiência de recursos.

2 PROJETADO E OTIMIZADO PARA O VMWARE NSX

A integração nativa de nossa solução sem agentes com a plataforma VMware NSX tornou sua infraestrutura virtual ainda mais eficiente e rentável. A partir de agora, sua infraestrutura VMware vSphere com NSX e as camadas de segurança trabalham em conjunto, proporcionando novos níveis de automação e segurança direcionada por políticas. Isso inclui o aprimoramento das operações por meio da proteção automatizada, fortalecida por funcionalidades de segurança granulares fornecidas rapidamente pela integração de políticas e marcas de segurança.

3 VISIBILIDADE E GERENCIABILIDADE EM NÍVEL EMPRESARIAL

O console de administração unificado permite que sua equipe de TI gerencie centralmente a segurança de todas as VMs, junto com os produtos de segurança da Kaspersky Lab em execução em sua infraestrutura física e seus dispositivos móveis.

Ao facilitar o gerenciamento de ambientes híbridos, que combinam plataformas virtuais, físicas e móveis, a Kaspersky Lab permite que sua equipe implante projetos de virtualização no ritmo desejado, com menos pressão sobre os recursos de TI e um alcance menor dos erros humanos.

O Kaspersky Security for Virtualization fornece funcionalidades avançadas de segurança a ambientes corporativos híbridos desenvolvidos na plataforma VMware NSX e possibilita os melhores níveis de eficiência das operações, pois a solução não afeta o desempenho dos sistemas. A arquitetura sensível à virtualização da solução de segurança da Kaspersky Lab oferece um conjunto de ferramentas abrangente, que engloba tecnologias de proteção capazes de se integrar de modo eficaz e trabalhar com a infraestrutura de TI em nível central. As infraestruturas híbridas ganham benefícios adicionais pela operação conjunta com o Kaspersky Security for Virtualization.

Saiba mais em www.kaspersky.com/data-center-security

KASPERSKY lab