2020

kaspersky

Proteção comprovada e orquestração sem fronteiras para sua nuvem híbrida

Saiba mais em kaspersky.com #truecybersecurity

Kaspersky Hybrid Cloud Security

A virtualização tornou-se uma abordagem essencial para todas as empresas que desejam ser flexíveis e eficientes. A computação em nuvem é o próximo passo natural. Ela alivia as limitações de suporte a infraestruturas complexas e oferece níveis de eficiência antes impossíveis. Mas o processo de migração para a nuvem tem seus perigos e complicações, alguns novos e outros herdados do mundo físico.

O Kaspersky Hybrid Cloud Security oferece segurança unificada para todas as fases ou cenários de seu processo de migração para a nuvem. Adequado para cenários de migração para a nuvem e nativos da nuvem, ele protege suas cargas de trabalho físicas e virtualizadas, independentemente delas serem executadas no local, em um data center ou em uma nuvem pública. Como seus aplicativos foram criados considerando as especificidades de funcionamento de servidores e da virtualização, ele oferece uma proteção perfeitamente equilibrada contra as ameaças atuais e futuras mais avançadas sem afetar o desempenho do sistema.

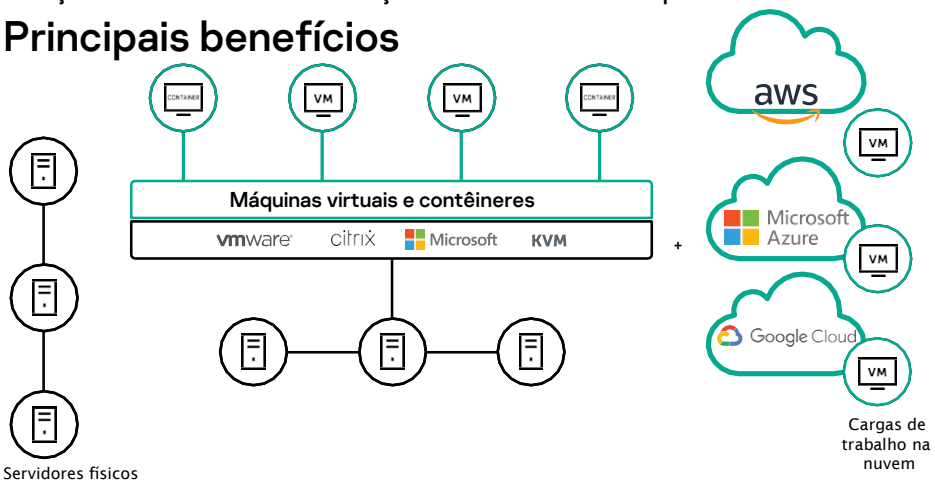
Maiores desafios relacionados à adoção da nuvem:

- A crescente complexidade da infraestrutura pode resultar em menor transparência
- É raro encontrar uma abordagem em vários níveis, fundamental para a proteção confiável, em um único produto
- A segurança pesada tradicional consome recursos valiosos do sistema
- A abordagem de silos e os controles distintos geram desafios adicionais para a segurança e administração
- Malware e ransomware atacam endpoints virtuais e físicos
- A não implementação de medidas de cibersegurança adequadas para a proteção de dados pessoais pode causar problemas legais.

Por que escolher o Kaspersky Hybrid Cloud Security?

- Projetado para cargas de trabalho físicas, virtuais e na nuvem
- Segurança integrada em vários níveis para todos os tipos de cargas de trabalho
- Segurança consistente, automatizada e ágil para as nuvens públicas do AWS, Azure e Google
- Ajuda na responsabilidade compartilhada com um conjunto completo de ferramentas de segurança
- Orquestração contínua da segurança em toda a sua nuvem híbrida
- A proteção mais testada e mais premiada, de acordo com vários prêmios e testes independentes[1]

Principais benefícios



Possibilita uma jornada de migração segura para a nuvem sem comprometer os níveis de proteção

- Tecnologias patenteadas e nosso premiado mecanismo de cibersegurança protegem todas as suas cargas de trabalho, físicas, virtualizadas ou na nuvem.
- Proteção em tempo real e em várias camadas, alimentada por Machine Learning, protege seus dados, processos e aplicativos de ameaças emergentes.
- Uma abordagem holística de segurança de dados ajuda a reduzir os riscos legais e de reputação relacionados às regulamentações de proteção de dados.

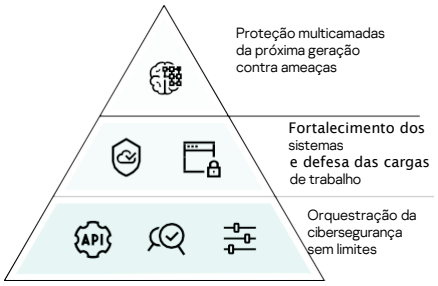
Garante que você aproveite seus recursos e investimentos ao máximo

- A proteção sem agentes e com agentes leves protege ativos virtualizados em redes regulares e definidas por software sem afetar o desempenho.
- A integração com a segurança nativa de nuvens públicas e gerenciadas ajuda a proteger seus aplicativos, sistemas operacionais, fluxos de dados e espaços de trabalho do usuário com a menor exigência de recursos possível.
- O gerenciamento com visualização única de recursos físicos e virtuais economiza tempo trabalho durante a adoção e manutenção.

1 Os testes referem-se a uma série de produtos da Kaspersky que têm como base as mesmas tecnologias de proteção contra ameaças utilizadas no Kaspersky Hybrid Cloud Security. Saiba mais em kaspersky.com/top3

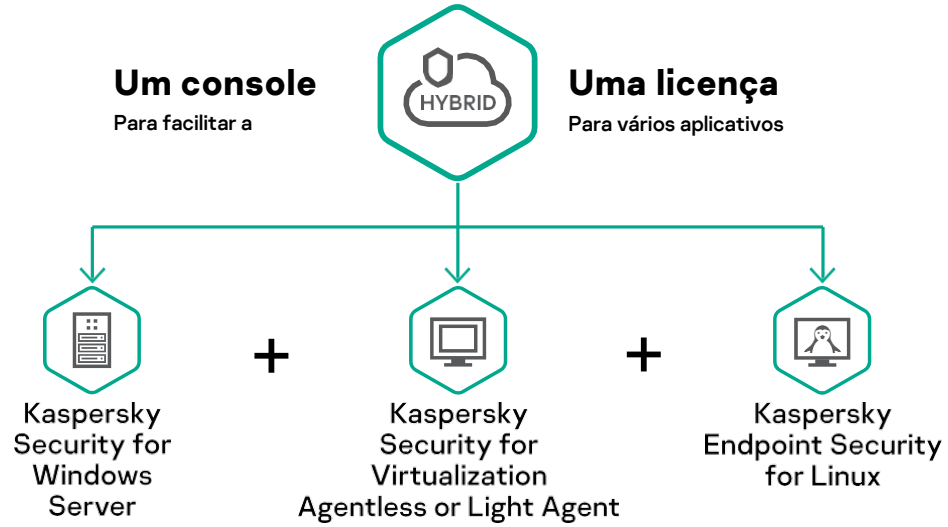
Recursos

Recurso	Descrição
Proteção contra ameaças em várias camadas **A proteção contra malware da próxima geração da Kaspersky incorpora várias camadas de segurança proativa capazes de bloquear a mais ampla variedade de ataques cibernéticos que ameaçam suas cargas de trabalho críticas para os negócios.**	
Inteligência global de ameaças	Fornece dados em tempo real sobre o estado do cenário de ameaças, mesmo conforme ele muda, garantindo sua proteção ininterrupta.
Machine Learning	O Big Data de inteligência de ameaças global é processado pela capacidade combinada dos algoritmos de Machine Learning e do conhecimento humano para proporcionar altos níveis de detecção comprovados com o mínimo de falsos positivos.
Proteção contra ameaças da Web e de e-mail	Possibilita o funcionamento seguro de áreas de trabalho virtuais e remotas, protegendo-as de ameaças baseadas em e-mail e na Web
Inspeção de logs	Verifica os arquivos de log internos para proporcionar a higiene operacional ideal.
Análise de comportamento	Monitora aplicativos e processos, oferecendo proteção contra ameaças avançadas, inclusive malware sem corpo ou baseado em scripts.
Mecanismo de neutralização	Se necessário, reverte todas as alterações maliciosas feitas nas cargas de trabalho na nuvem.
Prevenção de exploits	Oferece proteção eficaz contra o lançamento de ataques e, ao mesmo tempo, garante perfeita compatibilidade com os aplicativos protegidos, tudo com impacto mínimo sobre o desempenho.
Funcionalidade anti-ransomware	Protege cargas de trabalho virtualizadas contra tentativas de reter dados críticos para os negócios para fins de resgate, revertendo os arquivos afetados para seu estado pré-criptografado e bloqueando a criptografia iniciada remotamente.
Proteção contra ameaças de rede	Detecta e impede invasões baseadas na rede dos ativos em nuvem.
Proteção de contêineres	Garante que não seja possível transferir as infecções para sua infraestrutura de TI híbrida por meio de contêineres comprometidos do Docker ou Windows.
O fortalecimento do sistema incrementa a resiliência	
Controle de Aplicativos	Permite travar todas as suas cargas de trabalho na nuvem híbrida no modo de Negação Padrão para o fortalecimento ideal do sistema, sendo possível limitar a execução apenas de aplicativos legítimos e confiáveis.
Controle de Dispositivos	Especifica quais dispositivos virtualizados podem acessar cargas de trabalho individuais na nuvem.
Controle da Web	Regula o uso de recursos da Web por áreas de trabalho virtuais e remotas para reduzir os riscos e incrementar a produtividade.
Sistema de Prevenção de Invasões Baseado em Host	Atribui categorias confiáveis aos aplicativos executados, restringindo seu acesso a recursos críticos e limitando suas funcionalidades.
Monitoramento de Integridade de Arquivos	Ajuda a garantir a integridade de componentes críticos do sistema e outros arquivos importantes.
Avaliação de Vulnerabilidades e Gerenciamento de Patches	Centraliza e automatiza tarefas essenciais de segurança, configuração do sistema e gerenciamento, como avaliação de vulnerabilidades, distribuição de patches e atualizações, gerenciamento de inventário e distribuição de aplicativos.
Visibilidade sem limites	
Gerenciamento unificado da segurança	O Kaspersky Security Center facilita a administração da segurança com visualização única de toda a infraestrutura, endpoints e servidores, no escritório, em seu data center e na nuvem.
API na nuvem	A perfeita integração com os ambientes públicos do AWS e Azure permite a descoberta da infraestrutura, a implementação automatizada de agentes de segurança e o gerenciamento baseado em políticas, além de facilitar o provisionamento da segurança e inventário.
Opções de gerenciamento flexível	Apresenta funcionalidades multilocatário, gerenciamento de contas baseado em permissões e controle de acesso baseado em funções, proporcionando flexibilidade ao mesmo tempo que mantém os benefícios da orquestração unificada em um único servidor.
Integração com SIEMs	Em infraestruturas com uma TI mais madura, é possível usar os sistemas de gerenciamento de informações de segurança como uma janela unificada para diferentes aspectos da cibersegurança da empresa em toda a rede de TI híbrida.



Proporciona visibilidade e controle consistentes, independentemente da configuração de sua infraestrutura híbrida

- Provisionamento facilitado dos serviços de segurança e operações baseadas em políticas são ativados em toda a nuvem híbrida.
- A gerenciabilidade e a orquestração da segurança são operadas ininterruptamente nas várias nuvens.
- Visibilidade total, controle e proteção holística de todas as cargas de trabalho, em todos os locais, contra as ameaças mais avançadas.



O Kaspersky Hybrid Cloud Security oferece várias tecnologias de segurança premiadas e reconhecidas pelo setor para respaldar e simplificar a transformação de seu ambiente de TI. Ele protege sua migração do físico para o virtual e para a nuvem, enquanto a visibilidade e a transparência garantem a orquestração impecável da segurança.

Segurança unificada para todas as nuvens:

Nuvens públicas
- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform

Data centers privados
- Vmware NSX
- Microsoft Hyper-V
- Hipervisor Citrix
- KVM
- Proxmox

Ambientes de VDI
- Vmware Horizon
- Citrix Virtual Apps and Desktops

Servidores físicos
- Windows
- Linux

Áreas de trabalho físicas:
- Windows
- Linux

Notícias sobre ameaças cibernéticas:
www.securelist.com
Notícias sobre segurança de TI:
business.kaspersky.com
Cibersegurança para PMEs:
kaspersky.com/business
Cibersegurança para corporações:
kaspersky.com/enterprise

www.kaspersky.com.br

Nós somos comprovados. Somos independentes. Somos transparentes. Temos o compromisso de construir um mundo mais seguro, onde a tecnologia melhora nossas vidas. Por isso, nós a protegemos. Para que todos possam aproveitar as infinitas oportunidades que ela proporciona. Garanta a cibersegurança para um futuro mais seguro.

Saiba mais em kaspersky.com/transparency

Proven. Transparent. Independent.