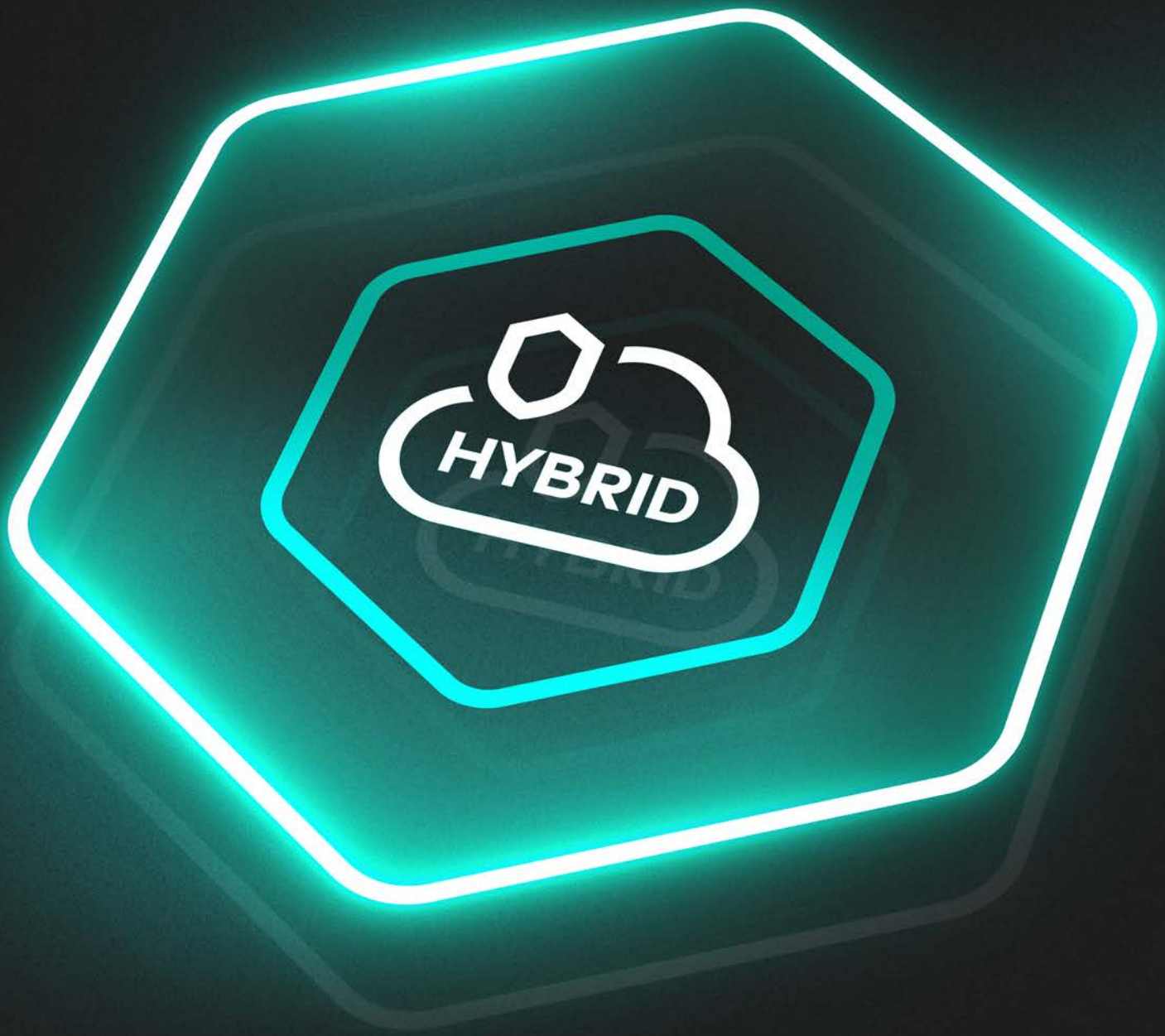


Kaspersky Hybrid Cloud Security

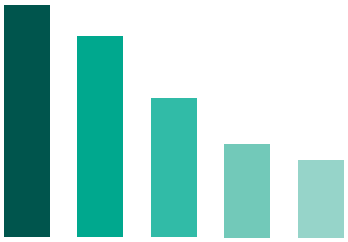
kaspersky PREPARADOS PARA O FUTURO

O foco dos negócios de hoje na transformação digital está desencadeando a rápida adoção da nuvem. Por um lado, essas iniciativas trazem muitas vantagens para as empresas, incluindo maior eficiência. Por outro lado, as infraestruturas tornam-se mais complexas, gerando preocupações significativas em termos de risco de segurança, governança, recursos humanos, otimização de desempenho, novas regulamentações e gastos. O Kaspersky Hybrid Cloud Security resolve todos esses desafios.

Proteção nativa da nuvem e o melhor desempenho comprovados para seus ambientes híbridos

O Kaspersky Hybrid Cloud Security torna a adoção da nuvem, a transformação digital e os negócios em geral mais seguros e eficientes. Este produto único protege toda a sua infraestrutura híbrida, mitigando riscos, reduzindo o consumo de recursos de virtualização e oferecendo suporte à conformidade regulatória. O Kaspersky Hybrid Cloud Security oferece maior visibilidade e gerenciamento simplificado, enquanto poupa tempo valioso e recursos orçamentários para você e sua equipe. A segurança se torna uma preocupação a menos – deixando você livre para se concentrar em outros aspectos da jornada de transformação digital.

Principais desafios da nuvem



- Segurança **81%**
- Gerenciamento de gastos com a nuvem **79%**
- Governança e conformidade **75%**
- Gerenciamento de múltiplas nuvens **72%**
- Migração para a nuvem **71%**

De acordo com o Flexera State of the Cloud Report 2021

A melhor proteção da categoria projetada para lidar com os riscos de segurança do ambiente híbrido

- A proteção em multicamadas contra ameaças combate proativamente diversos ciberataques, incluindo malware, phishing e muito mais.
- Os algoritmos de Machine Learning viabilizados por expertise humana proporcionam os níveis mais altos de detecção com o mínimo de falsos positivos.
- Dados de inteligência de ameaças em tempo real ajudam na defesa contra as explorações mais recentes.

Uma abordagem nativa da nuvem para garantir o melhor desempenho de segurança para infraestruturas híbridas

- O mecanismo de cibersegurança protege toda a infraestrutura híbrida, seja qual for a carga de trabalho: física, virtualizada ou baseada em nuvens privadas, públicas e híbridas.
- Uma abordagem independente de plataforma combinada com integração nativa torna as nuvens públicas totalmente habilitadas para DevOps.
- Agentes leves otimizados para cada SO reduzem com eficiência o consumo de recursos de virtualização em até 30%, liberando-os para uso em outras operações comerciais.

Rentabilidade e gestão conveniente para uma migração para a nuvem sem problemas

- Um modelo de licenciamento flexível significa que você escolhe somente os recursos necessários, obtendo o máximo de benefícios do seu investimento em segurança.
- Um console na nuvem unificado simplifica o gerenciamento da segurança de toda a sua infraestrutura, poupando recursos valiosos da equipe de TI.
- O inventário de infraestrutura de nuvem simples e o provisionamento de segurança automatizado, independentemente da localização dos agentes, contribuem para a visibilidade máxima.

Segurança em conformidade com os requisitos de indústrias altamente regulamentadas

- Adaptável e multifacetado, este produto foi projetado para permitir e oferecer suporte contínuo à conformidade regulatória completa, por meio de tecnologias que vão desde o fortalecimento do sistema e autodefesa do agente até a avaliação de vulnerabilidades e gerenciamento automatizado de patches.
- A ampla variedade de recursos proporciona conformidade e adaptação ao cenário de risco, mantendo sua segurança continuamente em dia com a legislação vigente.

Recursos

Proteção contra ameaças em vários níveis

Inteligência Global de Ameaças	Coleta dados em tempo real sobre o estado do cenário de ameaças, mesmo quando ele muda.
Aprendizado de máquina	Capacita o big data da inteligência global de ameaças com algoritmos de Machine Learning e expertise humana.
Proteção de ameaças da Web e e-mail	Protege desktops remotos e virtuais contra ameaças de e-mails e da Web.
Inspeção de logs	Verifica arquivos de log para a melhor segurança operacional.
Análise comportamental	Protege contra ameaças avançadas, incluindo malware imaterial ou baseado em script, por meio do monitoramento de aplicativos e processos.
Mecanismo de neutralização	Desfaz quaisquer alterações maliciosas feitas dentro de cargas de trabalho na nuvem caso sejam necessárias.
Prevenção contra exploits	Oferece proteção eficaz contra a penetração de ameaças em total compatibilidade com aplicativos protegidos, resultando em um impacto mínimo no desempenho.
Recurso anti-ransomware	Protege os dados críticos dos negócios de qualquer tentativa de pedido de resgate, incluindo o bloqueio de criptografia iniciada remotamente e a reversão de arquivos afetados para seu estado pré-criptografado.
Proteção contra ameaças à rede	Detecta e impede intrusões nos seus recursos localizados na nuvem.
Proteção de contêineres	Evita que infecções sejam transportadas para a infraestrutura de TI híbrida por meio de contêineres comprometidos.

Aumento de segurança do sistema que melhora a resiliência

Controle de Aplicativos	Permite o bloqueio de todas as suas cargas de trabalho de nuvem híbrida no modo Rejeição Padrão para a melhor proteção de sistema e a limitação do alcance de aplicativos em execução para somente aqueles legítimos e confiáveis.
Controle de dispositivos	Especifica quais dispositivos virtualizados podem acessar a cargas de trabalhos individuais na nuvem.
Controle da Web	Regula o uso de recursos da web por desktops remotos e virtuais, diminuindo riscos e turbinando a produtividade.
Sistema de Prevenção de Invasões com Base no Host (HIPS)	Designa categorias de confiança para aplicativos iniciados, restringindo seu acesso a recursos críticos e limitando suas capacidades.
Monitoramento da integridade dos arquivos	Ajuda a garantir a integridade de componentes de sistemas críticos e outros arquivos importantes.
Verificação de vulnerabilidades e gerenciamento de correções	Centraliza e automatiza segurança essencial, configuração de sistema e gerenciamento de tarefas, como avaliação de vulnerabilidade, correção e atualização de distribuição, gerenciamento de inventário e implementações de aplicativos.

Visibilidade sem barreiras

Gerenciamento de segurança unificado	A proteção de endpoints e servidores para toda a infraestrutura pode ser gerenciada por meio de um console – no escritório, no data center e na nuvem.
API de nuvem	Integração perfeita com ambientes de nuvem pública possibilita descoberta de infraestrutura, implantação automatizada de agentes de segurança e gestão baseada em políticas, além de facilitar o provisionamento de segurança e inventário.
Opções de gerenciamento flexível	Os recursos de multilocatário, gestão de contas baseada em permissões e controle de acesso baseados em cargas oferecem flexibilidade enquanto mantém os benefícios de orquestração unificada de um só servidor.
Integração com SIEM	Permite a integração do produto com o Security Information and Management System, reunindo diferentes aspectos da segurança cibernética corporativa em um só lugar – em toda a rede híbrida de TI.

Por que escolher o Kaspersky Hybrid Cloud Security?

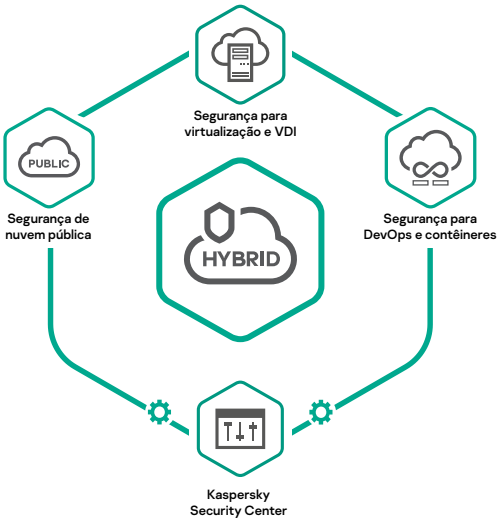
30%

das economias potenciais em recursos de hardware de virtualização em comparação com o uso de uma solução tradicional de segurança de endpoint.

TOP3

desempenho sustentável excelente. No ano passado, os produtos Kaspersky tiveram um desempenho excepcional em vários testes independentes, alcançando os 57 primeiros lugares e 63 conclusões nos três primeiros lugares (saiba mais em kaspersky.com/top3).

Um produto para todas as necessidades de segurança na nuvem



Um produto | **Um console** | **Uma licença**

Avaliações de clientes

"Esta solução ajuda a proteger ambientes virtuais e em nuvem, sem afetar o desempenho do sistema ou interromper a experiência do usuário."

"Ótima maneira de combinar todas as soluções de segurança em uma licença."

"Não há necessidade de instalar software antivírus adicional e outros agentes."

"Solução em nuvem centralizada para proteção de dados. Tudo em um só lugar."

"A proteção é aplicada instantaneamente a todas as VM, pois você não precisa baixar novas atualizações."

"A solução ideal que não requer um longo treinamento de administradores."

Trechos de avaliações da Amazon e Gartner

Solicite uma demonstração

www.kaspersky.com.br