



Recursos de rede e de
segurança confiáveis
em uma só solução

Kaspersky SD-WAN

kaspersky preparados
para o futuro

Introdução

Para a maioria das empresas da atualidade, a continuidade dos negócios depende diretamente da confiabilidade da rede e do acesso ininterrupto aos recursos da web. Com várias filiais, equipes distribuídas, recursos na nuvem e funcionários trabalhando remotamente, se tornou cada vez mais complexo fornecer e gerenciar a segurança, mantendo uma infraestrutura de rede adequada. Essas condições exigem uma abordagem flexível que atende às demandas em constante evolução da sua empresa.

Desafios do cliente ao usar canais WAN tradicionais

Longo tempo de lead para conectar novos locais, e consumo intensivo de recursos humanos para escalar a infraestrutura em geral

Gerenciamento de infraestruturas complexas e escassez de especialistas qualificados

Ameaças de segurança e falta de integridade de segurança geral entre filiais

Alto custo operacional de link WAN, conexão fraca ou problemas de utilização

Falta de confiabilidade geral da infraestrutura e desempenho inefficiente dos aplicativos

Muitos incidentes de TI ocorrem, inclusive relacionados a erros humanos.

Facilite sua vida com o Kaspersky SD-WAN

O Kaspersky SD-WAN cria redes seguras e tolerantes a falhas através do gerenciamento unificado, solucionando os desafios associados às WANs tradicionais. A solução permite a você usar diversos canais de comunicação, otimizar conexões em nuvem, aprimorar a segurança e melhorar o desempenho de aplicações, além de acelerar a implementação de novos serviços.

O Kaspersky SD-WAN fornece recursos para gerenciar a rede de transporte e integrar ferramentas de transferência de dados (como routers virtuais), bem como serviços de análise e de segurança por meio do Gerenciador de Funcionalidades da Rede Virtual (VNFs) e o orquestrador dentro de sua arquitetura. Esta abordagem ajuda você a criar com facilidade o seu próprio ecossistema de segurança de rede, e a implementar uma abordagem do tipo SASE (Secure Access Service Edge).

Secure Access Service Edge (SASE)

O termo SASE refere-se a sinergia de serviços de segurança e de rede, que tem como objetivo fornecer redes confiáveis e ágeis, deixando de lado soluções de segurança diferentes para adotar uma segurança unificada disponível em nuvens privadas ou públicas. Toda a rede da empresa está protegida, independentemente de onde os usuários estão, ou como se conectam.

Fácil escalabilidade

Conecte novas localizações com uma experiência de zero-touch, atendendo às demandas em constante mudança dos negócios

Segurança centralizada

Implemente controle de tráfego virtualizado e ferramentas de segurança via gerenciador VNF

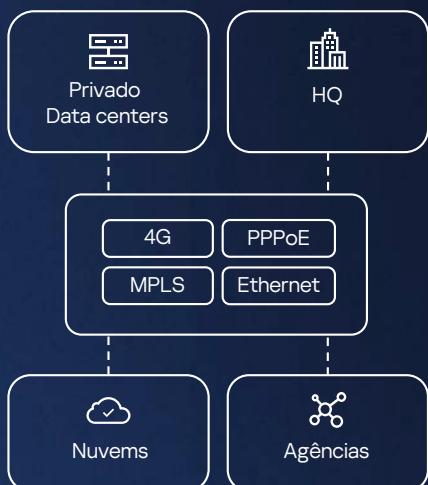
Otimização de custos

Reduza custos de infraestrutura, convergindo canais de comunicação separados e funcionalidades de rede

Gerenciamento conveniente

Gerencie toda a sua rede via um único console, modificando políticas de segurança e regras de filtragem de tráfego

Recursos principais



Rede confiável para todas as filiais

Use quaisquer canais de comunicação

A solução fornece acesso para todos os recursos corporativos (escritórios, nuvens públicas e privadas e data centers) com diversos canais de comunicação: MPLS, Ethernet, 4G e outros canais a cabo e sem fio.

Conecte instantaneamente novos locais

Equipamentos no Local do Cliente (CPE) torna a conexão com novos locais harmoniosa e rápida, sem configurações adicionais, graças ao Provisionamento Zero Touch (ZTP), reduzindo o tempo de implementação de horas para apenas alguns minutos.

Desfrute de uma transferência de dados sem interrupções

A solução permite configurar túneis dinâmicos entre CPE, gerenciar e priorizar tráfego de aplicações, otimizar transferência de dados, e orquestrar eficientemente as funções de rede.



Um único console de gerenciamento

Gerencie toda a sua rede

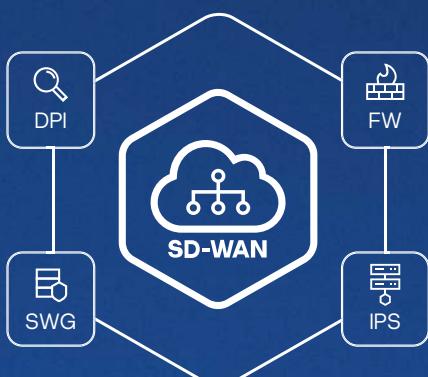
Uma interface da web unificada permite gerenciar toda a rede diretamente do orquestrador ou da Plataforma Única de Gerenciamento Aberto (OSMP): configurar CPE, criar regras de filtragem de tráfego e políticas de segurança, além de definir SLAs para serviços.

Crie e visualize sua infraestrutura

Uma ferramenta gráfica permite a você planejar e visualizar toda a sua infraestrutura da rede, facilitando a integração de serviços. Basta arrastar e soltar funções de rede virtual que podem ser inicializadas imediatamente.

Aproveite de dashboards informativos

O estado de toda a infraestrutura está sob seu controle, incluindo CPE, funções virtualizadas e recursos físicos.



Segurança unificada

Política única de segurança

A solução fornece segurança para filiais, usando overlay de VPN, configurações de dispositivo centralizadas, políticas de segurança e regras de tráfego, disseminando-as em toda a rede WAN.

Conecte ferramentas de segurança com facilidade

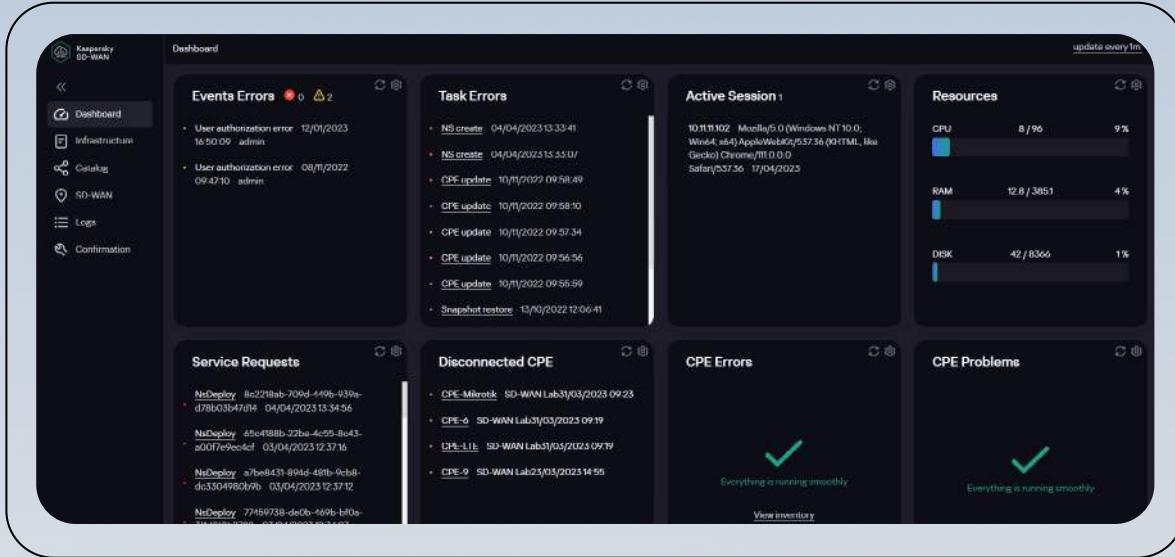
A virtualização de funções de rede permite a você implementar controle de tráfego e ferramentas de segurança automaticamente, incluindo firewalls, gateways da web protegidos, e sistemas de prevenção de intrusão.

Arquitetura flexível

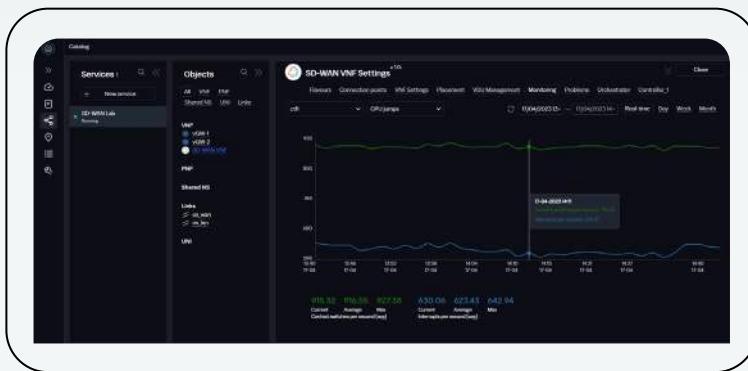
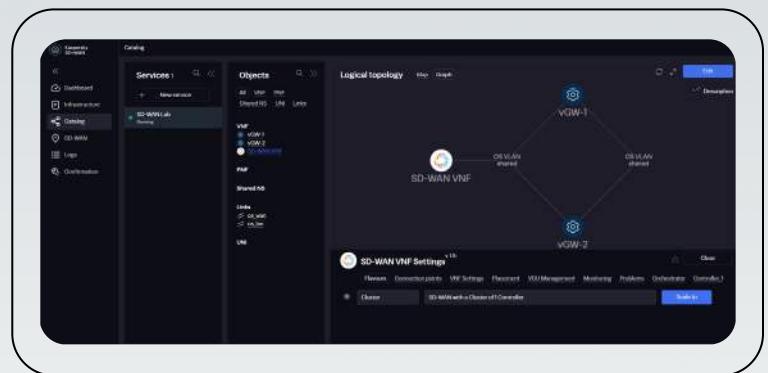
A solução permite integrar facilmente ferramentas de segurança de diferentes fornecedores, graças ao gerenciador Funções de Rede Virtuais (VNFs) e o orquestrador dentro da sua arquitetura.

Interface da web conveniente e informativa

As informações mais cruciais sobre a solução e o status da sua rede são mostradas na tela principal



A ferramenta gráfica de fluxos de serviço com recursos abrangentes



Uso de recursos virtuais e do servidor, com base em uma ampla variedade de parâmetros

Arquitetura conceitual da solução

Segurança

Implementação automatizada de ferramentas de controle e de segurança de tráfego



Gerenciamento

Console unificado para gerenciamento:



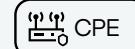
Opções de implementação do orquestrador e do controlador



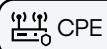
Orquestrador/ controlador



Nuvem pública



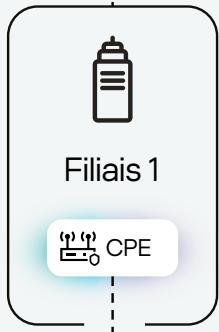
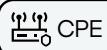
Data center



HQ



Filial principal

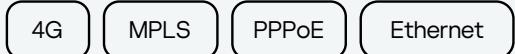


• • •



Canais de comunicação

Flexibilidade para escolher os canais de comunicação e suas combinações



Acesso

Acesso seguro a:



Configure automaticamente
o acesso aos recursos
corporativos

Implantar ambientes
de software (PaaS)

Níveis e recursos do Kaspersky SD-WAN

O Kaspersky SD-WAN está disponível em dois níveis: Standard e Advanced.

	Funcionalidades	Standard	Advanced
 Conexão e gerenciamento	Compatível com taxa de transmissão CPE de até 10 GB/s	●	●
	Gerenciamento de nuvem pública/privada ou no local	●	●
	Integração de gerenciamento da plataforma com a Plataforma Única de Gerenciamento Aberto (OSMP)	●	●
	Organização da conectividade do CPE com o controlador por meio de portas LAN e WAN	●	●
	Compatível com tecnologias Hub e Spoke, Full Mesh e Partial Mesh	●	●
	Políticas SLA para aplicativos	●	●
	Roteamento dinâmico (BGP, OSPF)	●	●
	Compatível com VRF Lite	●	●
	DPI integrado	●	●
 Serviços SD-WAN	Firewall Stateful	●	●
	NAT (PAT, SNAT, DNAT)	●	●
	Provisionamento Zero Touch	●	●
	Controle de qualidade de canal em tempo real	●	●
	Gerenciamento de falhas de conectividade (CFM)	●	●
	Compatível com OpenFlow	●	●
	Otimização de canal (compatível com FEC e duplicação de pacotes)	●	●
	Roteamento baseado em políticas	●	●
	Compatível com serviços P2P, P2M, e L2/L3 VPN	●	●
 Funcionalidades de rede virtual	Compatível com criptografia de alta velocidade integrada	●	●
	Compatível com integração aos produtos Kaspersky	●	●
	ETSI MANO		●
	Compatível com VNFs de terceiros		●
	Gerenciamento do ciclo de vida da cadeia de serviços		●
 Serviços	Compatível com uCPE		●
	Compatibilidade multicast		●
	Compatível com PIM		●
	Compatibilidade multitenant		●

Licenciamento

A solução é licenciada por CPE com base nas taxas de transferência específicas. Você pode escolher dentre os nossos modelos recomendados da linha Kaspersky SD-WAN Edge Service Router (KESR) com várias interfaces.



Recursos de rede e de segurança confiáveis combinados em uma só solução



O vetor essencial da segurança unificada

O Kaspersky SD-WAN é um passo fundamental na construção de uma segurança unificada, além de uma rede distribuída confiável. Com o Kaspersky SD-WAN, você pode começar a desenvolver seu Secure Access Service Edge (SASE) imediatamente.

A equipe da Kaspersky tem um histórico imbatível de experiência em cibersegurança, e nossos produtos já foram avaliados como as soluções de segurança mais eficazes em mais de 700 testes independentes. Ao mesmo tempo que desenvolvemos ativamente as nossas soluções de segurança de rede, pretendemos aumentar a proteção dos clientes através de capacidades Secure Access Service Edge (SASE).

É muito fácil e rápido conectar o Kaspersky SD-WAN

1

Entrega de CPE para a filial

2

Conexão de CPE à rede

3

Para uso imediato!

O desenvolvimento de software seguro é a base do Kaspersky SD-WAN

O Kaspersky SD-WAN, assim como outros produtos da Kaspersky, é desenvolvido em conformidade com a metodologia SSDLC (Ciclo de Vida de Desenvolvimento de Software Seguro).

A Kaspersky Threat Research é um dos nossos cinco centros de especialização, cujos especialistas estão envolvidos na redução dos riscos associados às vulnerabilidades nos nossos produtos.

Saiba mais

Threat Research





Kaspersky SD-WAN

Saiba mais