Reliable network and security capabilities rolled into one

Kaspersky SD-WAN

kaspersky bring on the future

Introduction

Kaspersky SD-WAN is designed to build fault-tolerant and secure networks with unified management – essential for today's distributed businesses. The solution helps to protect your business continuity, enhances productivity and, therefore, supports you to easily achieve your digital transformation goals. Kaspersky SD-WAN is an essential step in building unified security on top of a reliable distributed network. With Kaspersky SD-WAN you can easily integrate security services and start to build SASE now.

SASE

Secure Access Service Edge (SASE) stands for network and security services synergy, which aims to provide agile and reliable networks, while shift left from different security solutions to unified security available from private or public clouds. The whole company network is secured, regardless of where your users are or how they connect to it.

Kaspersky SD-WAN is a business-focused solution

Use any available communication channels, including MPLS VPN, Ethernet, LTE, or any combination of them to connect new locations

Integrated security capabilities and real-time monitoring of all solution components, including DPI analysis to track the state of tunnels and applications

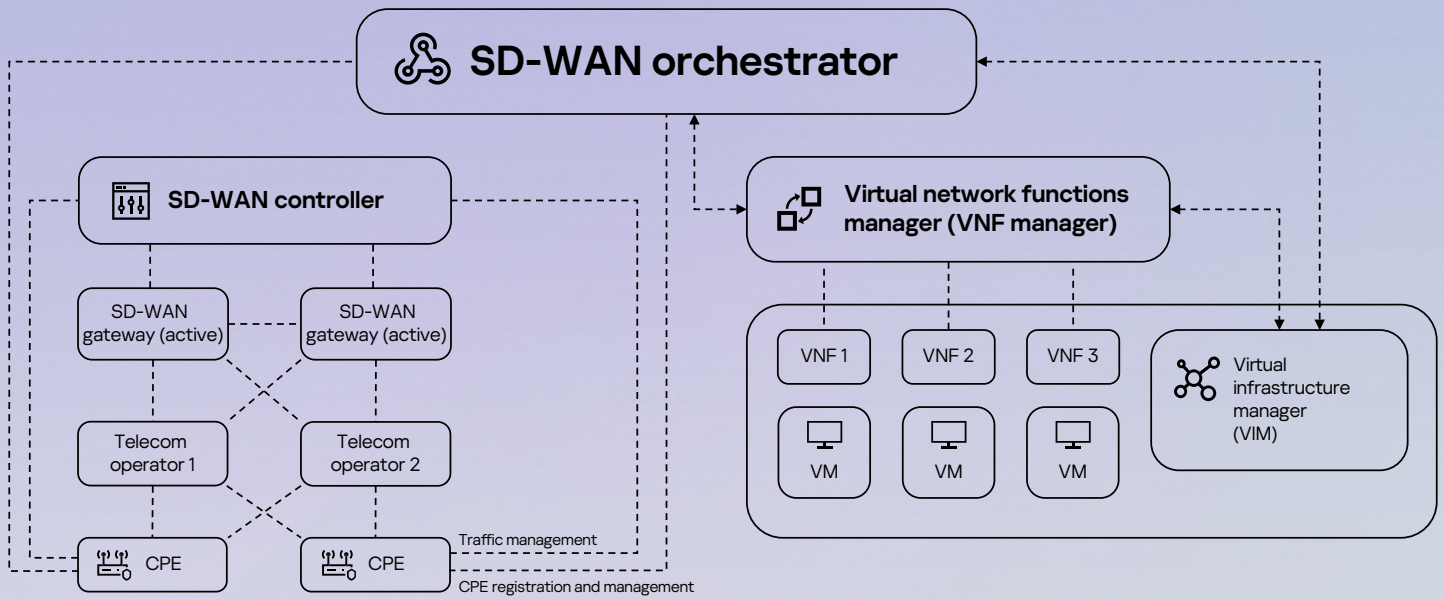
Zero Touch Provisioning connects branches to the corporate network without additional configuration – saving valuable staff time

Centralized management through a single web interface or API to quickly change solution settings and monitor a SD-WAN network of any size

Link management features and adherence to predefined SLAs for efficient performance of business-critical applications

Virtual Network Functions manager for easy deployment of Kaspersky's and third-party vendors' security tools

Solution architecture



Core components

The versatile architecture of Kaspersky SD-WAN supports the entire lifecycle of the solution, including centralized orchestration, automatic configuration, and monitoring.

SD-WAN orchestrator	Software component that manages SD-WAN controllers and controls the virtual infrastructure manager. The SD-WAN orchestrator provides a unified graphical interface and API interfaces for interaction with all solution components. It also collects, stores, and visualizes information on the state of the SD-WAN network, runs templates, assigns the settings of service chains, provides virtualization and control of resources, and manages licenses
SD-WAN controller	Software component that manages the SD-WAN CPE. The SD-WAN controller is responsible for managing traffic, exchanging routing information, and configuring the security policies and security settings of communication channels
Virtual infrastructure manager (VIM)	Third-party software responsible for configuring and managing the virtual infrastructure. OpenStack VIM is used by default in Kaspersky SD-WAN
Virtual network functions manager (VNF manager)	Software component that manages the lifecycle of virtual network functions. The VNF manager controls the installation, activation, scaling, updating and termination of virtual network functions
SD-WAN gateway	Network equipment deployed in the data center or HQ that aggregates SD-WAN tunnels. It is recommended to deploy SD-WAN gateways as a fault-tolerant pair
CPE	Customer premises equipment situated at branches for connecting communication channels and setting up tunnels to the SD-WAN gateway

Kaspersky SD-WAN capabilities

Capability	Description
Deployment	• On-premise • Clouds (private or public)
Virtual Network Functions (VNFs) and Network Management	• ETSI MANO • Integration of platform management with OSMP (Open Single Management Platform) • VNF support (Kaspersky as well as third-party vendors' products) • Service-chain lifecycle management • Active-Active Multimaster
CPE types	• Servers • Virtual CPE
Management	• Centralized management of CPE software versions and Kaspersky SD-WAN central components • Out-of-Band management for CPE (through underlay network without customer's tunnels)
SD-Branch	• LAN segmentation • Local services (DHCP and etc.) • DHCP static reservation • Local internet access • VNF support for Universal CPE (uCPE)
Supported communication channels	• 4G • MPLS • Ethernet • PPPoE
Supported network topologies	• Full mesh • Partial mesh • Hub-and-Spoke
Zero Touch Provisioning	• DHCP • Static • Two-factor authentication support • URL Auth
VPN/Overlay	• L2 Point-to-Point • Point-to-Multipoint • Multipoint-to-Multipoint • L3 VPN
Fault tolerance and redundancy	• High-availability cluster of central components • SD-WAN gateways redundancy (active/active) • CPE redundancy (VRRP)
LAN segmentation	Full 802.1q support for CPE LAN-ports (Access, Trunk, Q-in-Q)

Routing	• Static • BGP • OSPF • BFD • PIM • NAT (PAT, SNAT, DNAT) • VRF Lite • Multicast service support for SD-WAN network • Path MTU discovery support
WAN load balancing and fault tolerance	• Active/Standby • Active/Active • Bonding
Channel quality control	• SLA assessment based on traffic active probes • Link State Control • BFD
Channel optimization	• FEC • Packet Duplication
Quality of Service (QoS)	• Multilayer QoS • 8 queues per virtual service • DSCP support • SLA assessment (loss, jitter and delay) • QoS remapping support for CPE WAN interfaces • Policing and shaping support
L7 traffic routing	• Built-in DPI • Application aware routing • Application SLA
Security	• Stateful Firewall • Built-in High-Speed Encryption support • Encryption configuration per channel
Monitoring	• Monitoring of central components, CPEs, VNF • Network Test Access Point (TAP) • NetFlow

Licensing

Kaspersky SD-WAN is available in two tiers: Standard and Advanced.

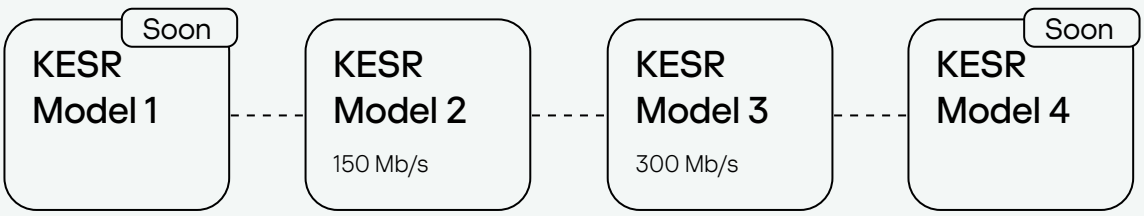
Kaspersky SD-WAN
Standard

Provides the tools for setting up and managing the network, and supports SD-WAN services and integration of Kaspersky products as virtual network functions.

Kaspersky SD-WAN
Advanced

Provides extended capabilities for virtual network functions, including those of third-party vendors, and includes Multicast and Multi-Tenancy support for services.

Each tier is licensing by CPE based on specific throughput. You can choose our recommended models from the Kaspersky SD-WAN Edge Service Router (KESR) line with various interfaces and performance.



KESR model line specifications

Model	Throughput	Key specifications	SKU
KESR Model 2	150 Mb/s	• 4 × Core CPU • 4 × LAN • 2 × Combo Ports • 2 × SFP+ • 2 × LTE	KESR-M2-GI
KESR Model 3	300 Mb/s	• 8 × Core CPU • 4 × LAN • 2 × Combo Ports • 2 × SFP+ • 2 × LTE	KESR-M3-GI

Secure Software Development is the foundation of Kaspersky SD-WAN

Kaspersky SD-WAN, like other Kaspersky's products, is developed in accordance with the SSDLC (Secure Software Development Lifecycle) methodology.

Kaspersky Threat Research is one of five Kaspersky expertise centers, whose specialists are engaged in reducing the risks associated with vulnerabilities in Kaspersky's products.

Learn more

Kaspersky SD-WAN

Learn more

www.kaspersky.com

#kaspersky
#bringonthefuture