



Reliable network and security  
capabilities rolled into one

# Kaspersky SD-WAN



# Introduction

For most companies today, business continuity directly depends on network reliability and uninterrupted access to web resources. With multiple branches, distributed teams, cloud resources, and remote employees, it becomes increasingly complicated to provide and manage security while properly maintaining your network infrastructure. These conditions require a versatile approach that meets the evolving demands of your business.

## Customer challenges when using traditional WAN channels

Long lead time to connect new locations, and labor-intensive infrastructure scaling in general

Managing complex infrastructures, and a shortage of qualified experts

Security threats and a lack of overall security integrity across branches

High WAN link operating costs, low bandwidth or utilization problems

A lack of overall infrastructure reliability and inefficient performance of applications

A large number of IT incidents, including those related to human errors

## Make your life easier with Kaspersky SD-WAN

Kaspersky SD-WAN builds fault-tolerant, secure networks with unified management, addressing the challenges associated with traditional WANs. The solution allows you to use diverse communication channels, optimize cloud connections, enhance the security and improve the performance of applications, and speed up implementation of new services.

Kaspersky SD-WAN delivers capabilities to manage the transport network and integrate data transfer tools (e.g. virtual routers) as well as analytical and security services through the Virtual Network Functions (VNFs) manager and the orchestrator within its architecture. This approach helps you to easily create your own network security ecosystem and implement a Secure Access Service Edge approach.

## Secure Access Service Edge (SASE)

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.

### Easy scalability

Connect new locations with a zero-touch experience to meet constantly changing business demands

### Centralized security

Automatically deploy virtualized traffic control and security tools through the VNF manager

### Cost optimization

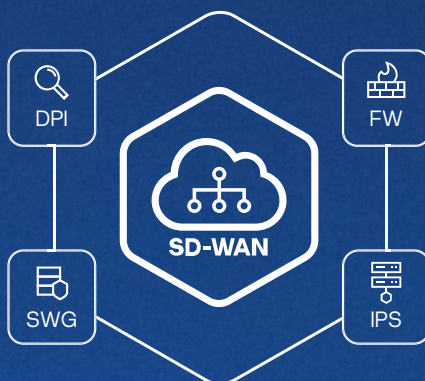
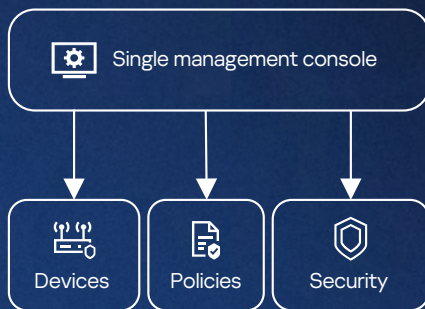
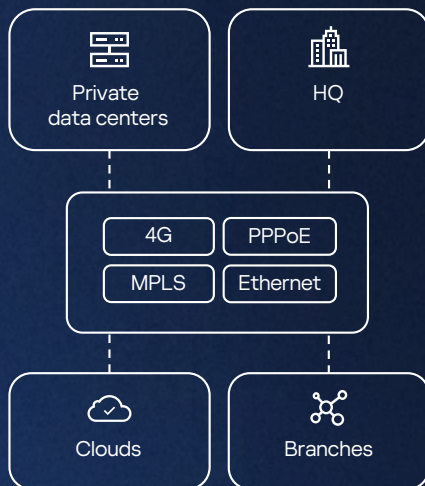
Reduce infrastructure costs, converging separate communication channels and network functions

### Convenient management

Manage your entire network from a single console, modifying security policies and traffic filtering rules



# Key features



## Reliable network for all branches

### Use any communication channels

The solution provides access to all company resources (offices, private and public clouds, and data centers) with diverse communication channels: MPLS, Ethernet, 4G and other wireless or wired channels.

### Instantly connect new locations

Customer Premises Equipment (CPE) makes connecting to new locations smooth and fast, without additional configurations through Zero-Touch Provisioning (ZTP), reducing deployment time to minutes.

### Enjoy smooth data transfer

The solution lets you configure dynamic tunnels between CPE, manage and prioritize application traffic, optimize data transfer, and efficiently orchestrate network functions.

## Single management console

### Manage your entire network

A unified web interface lets you manage the entire network from the orchestrator directly or from OSMP (Open Single Management Platform): configure CPE, create traffic filtering rules and security policies and define SLAs for services.

### Build and visualize your infrastructure

The convenient graphical builder lets you plan and visualize your network infrastructure while making integrating new services a breeze – just drag and drop virtual network functions that can then be launched immediately.

### Benefit from informative dashboards

The state of the entire infrastructure is in your control and at your fingertips, including CPE, virtualized functions, and physical resources.

## Unified security

### Single security policy

The solution provides security for branches using VPN overlay, centralized device configurations, security policies and traffic rules, pushing them out across the WAN.

### Easily connect security tools

The network functions virtualization lets you automatically deploy traffic control and security tools, including firewalls, secure web gateways and intrusion prevention systems.

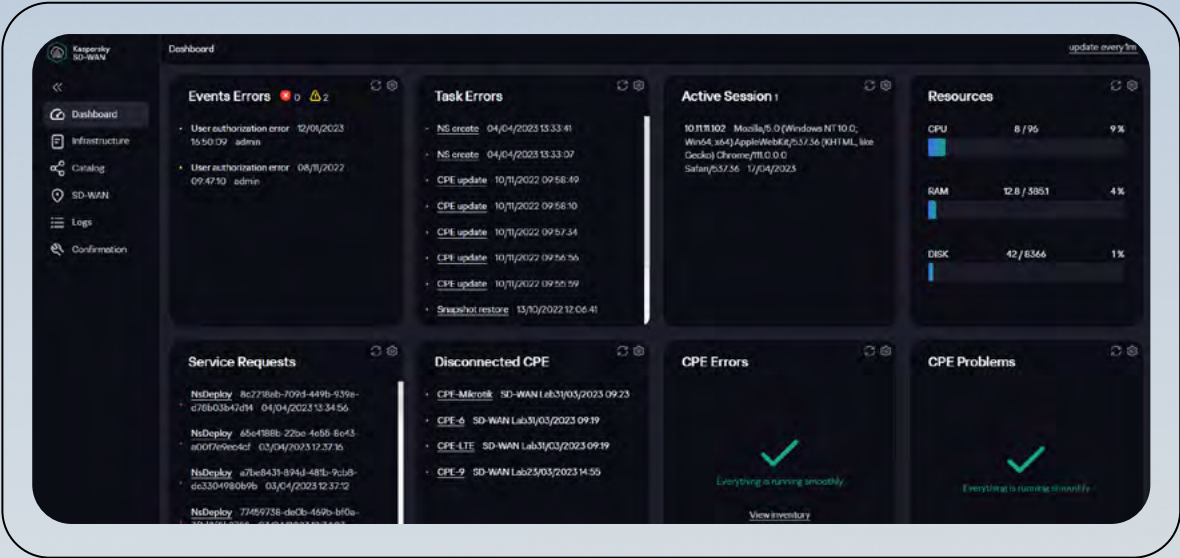
### Versatile architecture

The solution lets you easily integrate security tools from different vendors thanks to Virtual Network Functions (VNFs) manager and the orchestrator within its architecture.

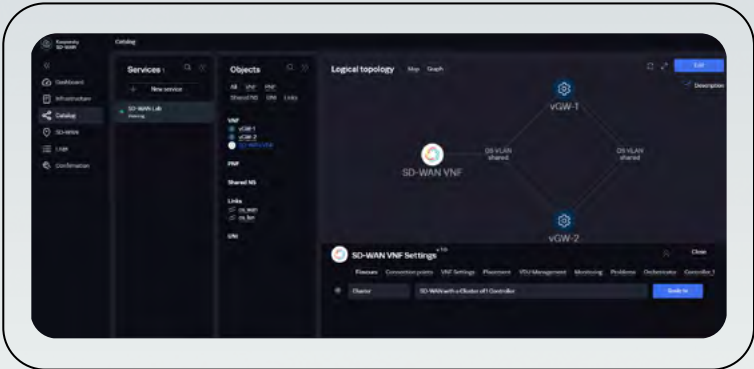


# Convenient and informative web interface

The key information about the solution and network status are on the main screen



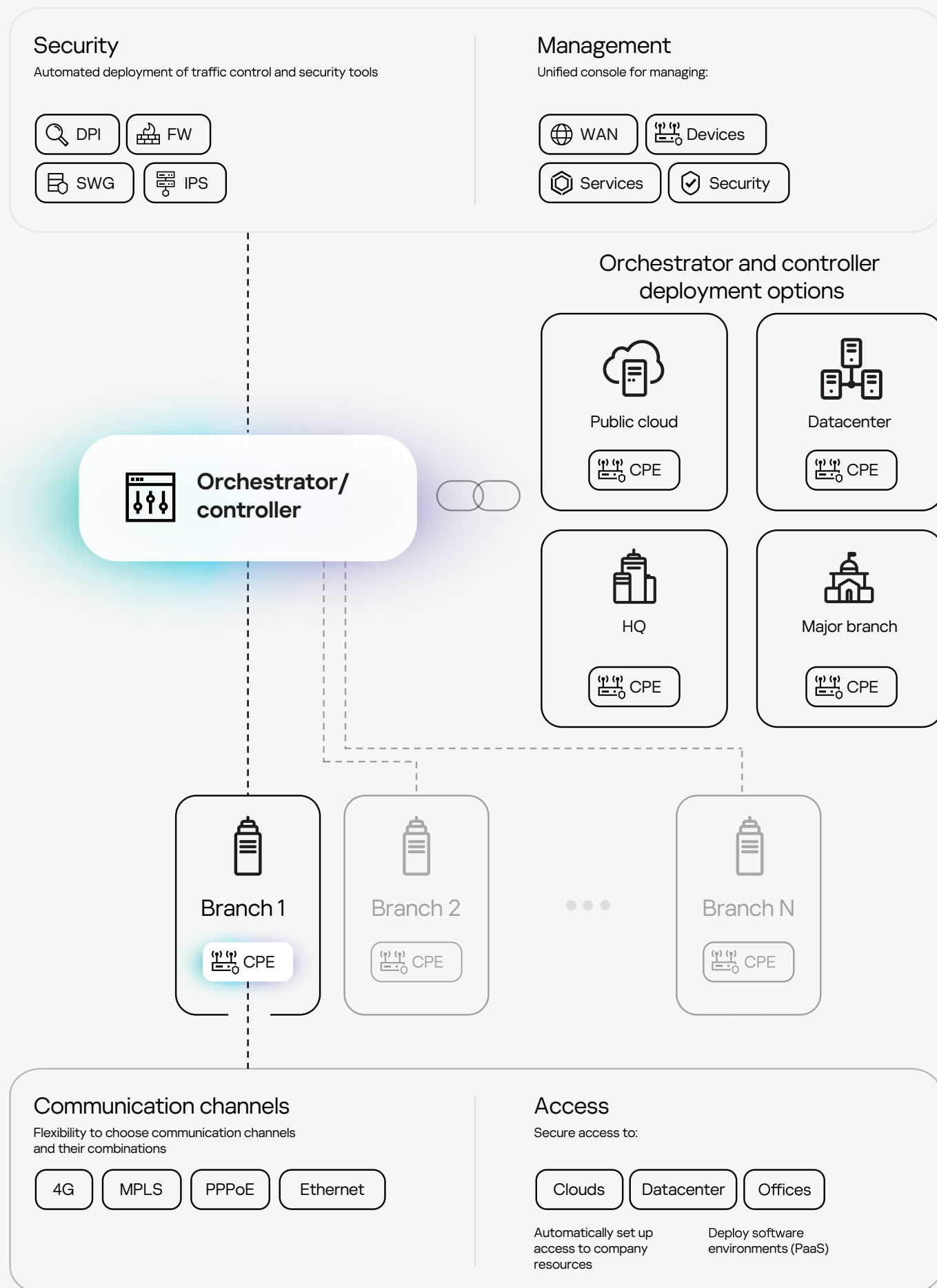
The convenient graphical builder of service chains with extensive capabilities



Usage of virtual and server resources based on a wide range of parameters







# Conceptual architecture of the solution





# Kaspersky SD-WAN tiers and capabilities

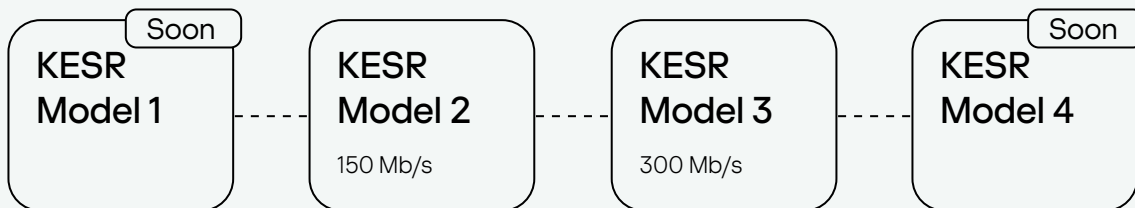
Kaspersky SD-WAN is available in two tiers: Standard and Advanced.

	Capabilities	Standard	Advanced
 Connection and management	Support for CPE throughput up to 10 Gb/s	●	●
	Management from private/public cloud or on-premise	●	●
	Integration of platform management with OSMP (Open Single Management Platform)	●	●
	Organization of CPE connectivity with the controller via LAN and WAN ports	●	●
	Support for Hub and Spoke, Full Mesh, and Partial Mesh topologies	●	●
	SLA policies for applications	●	●
	Dynamic routing (BGP, OSPF)	●	●
	VRF-Lite support	●	●
	Built-in DPI	●	●
	Stateful Firewall	●	●
	NAT (PAT, SNAT, DNAT)	●	●
 SD-WAN Services	Zero Touch Provisioning	●	●
	Real-time channel quality control	●	●
	Link State Control	●	●
	Support for OpenFlow	●	●
	Channel optimization (FEC and Packet Duplication support)	●	●
	Policy-Based Routing (PBR)	●	●
	Support for P2P, P2M, and L2/L3 VPN services	●	●
	Support for built-in high-speed encryption	●	●
 Virtual network functions	Support for integration of Kaspersky products	●	●
	ETSI MANO		●
	Support for third-party VNFs		●
	Service chain lifecycle management		●
	uCPE support		●
 Services	Multicast support		●
	PIM support		●
	Multi-Tenancy support		●



# Licensing

The solution 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.



## Reliable network and security capabilities rolled into one



### The transport backbone of unified security

Kaspersky SD-WAN is an essential step in building unified security on top of a reliable distributed network. With Kaspersky SD-WAN you can start to build Secure Access Service Edge (SASE) now.

The Kaspersky team has an unmatched track record of cybersecurity expertise, and our products have been evaluated as the most effective security solutions in more than 700 independent tests. While actively developing our network security solutions, we aim to increase customers' protection through Secure Access Service Edge (SASE) capabilities.

### It's quick and easy to connect Kaspersky SD-WAN

- 1 Deliver CPE to the branch
- 2 Connect CPE to the network
- 3 It's ready to use!

## 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.

Threat Research



[Learn more](#)





# Kaspersky SD-WAN

[Learn more](#)

[www.kaspersky.com](https://www.kaspersky.com)

© 2025 AO Kaspersky Lab.  
Registered trademarks and service marks are the property  
of their respective owners.

#kaspersky  
#bringonthefuture