



Güvenilir ağ ve güvenlik
kabiliyetleri bir arada

Kaspersky SD-WAN

kaspersky geleceği
yakalayın

Giriş

Günümüzde çoğu şirket için işletme sürekliliği doğrudan ağ güvenilirliğine ve web kaynaklarına kesintisiz erişime bağlıdır. Birden fazla şube, dağınık ekipler, bulut kaynakları ve uzaktan çalışanlar söz konusu olduğunda, ağ altyapınızı düzgün bir şekilde korurken güvenliği sağlamak ve yönetmek giderek daha karmaşık hale geliyor. Bu koşullar, işletmenizin artan taleplerini karşılayan çok yönlü bir yaklaşım gerektirir.

Geleneksel WAN kanallarını kullanırken müşterilerin karşılaştığı zorluklar

Yeni lokasyonları bağlamak için uzun tedarik süresi ve genel olarak yoğun işgücü gerektiren altyapı ölçeklendirmesi

Karmaşık altyapıların yönetilmesi ve kalifiye uzman eksikliği

Güvenlik tehditleri ve şubeler üzerinde genel güvenlik bütünlüğü eksikliği

Yüksek WAN bağlantısı işletim maliyetleri, düşük bant genişliği veya kullanım sorunları

Genel altyapı güvenilirliğinin eksikliği ve verimsiz uygulama performansı

İnsan hatalarıyla ilgili olanlar da dahil olmak üzere birçok BT olayı

Kaspersky SD-WAN ile hayatınızı kolaylaştırın

Kaspersky SD-WAN, geleneksel WAN'larla ilişkili zorlukları ele alarak birleştirilmiş yönetim ile güvenli, hatadan etkilenmeyen ağlar oluşturur. Bu çözüm, farklı iletişim kanallarını kullanmanıza, bulut bağlantılarını optimize etmenize, güvenliği artırmanıza, uygulamaların performansını geliştirmenize ve yeni hizmetlerin uygulanmasını hızlandırmanıza izin verir.

Kaspersky SD-WAN, mimarisindeki Sanal Ağ İşlevleri (VNF'ler) yöneticisi ve orkestratör aracılığıyla analitik ve güvenlik hizmetlerinin yanı sıra transfer ağını yönetme, veri transferi araçlarını (ör. sanal yönlendiriciler) entegre etme kabiliyetleri sunar. Bu yaklaşım, kendi ağ güvenliği ekosisteminizi kolayca oluşturmanıza ve bir Secure Access Service Edge (Güvenli Erişim Hizmet Ayrıtı) yaklaşımını uygulamanıza yardımcı olur.

Secure Access Service Edge (SASE)

SASE, ağ ve güvenlik hizmetleri sinerjisi anlamına gelir ve farklı güvenlik çözümlerinden özel veya genel bulutlardan kullanılabilen birleşik güvenliğe geçilirken çevik ve güvenilir ağlar sağlamayı amaçlar. Kullanıcılarınız nerede olursa olsun veya ağa nasıl bağlanırsa bağlansın, tüm şirket ağı güvence altındadır.

Kolay ölçeklenebilirlik

Sürekli değişen işletme gereksinimlerini karşılamak için yeni lokasyonları el değmeden bağlayın

Merkezi güvenlik

VNF yöneticisiyle sanallaştırılmış trafik kontrolü ve güvenlik araçlarını otomatik olarak devreye alın

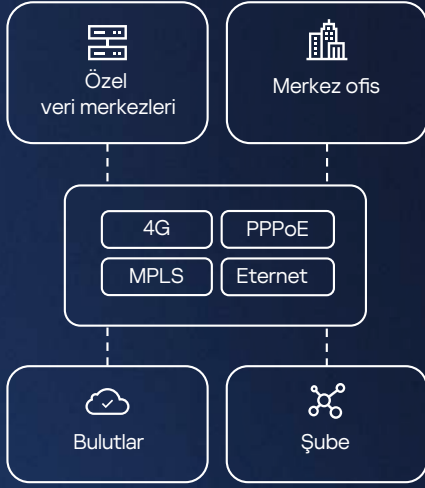
Maliyet optimizasyonu

Ayrı iletişim kanallarını ve ağ fonksiyonlarını birleştirerek altyapı maliyetlerini azaltın

Kolay yönetim

Güvenlik politikalarını ve akış filtreleme kurallarını modifiye ederek tüm ağını tek bir konsoldan yönetin

Temel özellikler



Tüm şubeler için güvenilir ağ

Tüm iletişim kanalını kullanın

Bu çözüm, MPLS, Ethernet, 4G ve diğer kablosuz veya kablolu iletişim kanalları gibi farklı iletişim kanalları ile tüm şirket kaynaklarına (ofisler, özel ve genel bulutlar ve veri merkezleri) erişim sağlar.

Yeni lokasyonlara anında bağlanın

Müşteri Tarafı Cihazları (CPE), devreye alma süresini dakikalara indirerek El Değmeden Tedarik (ZTP) ile ek yapılandırma olmadan yeni lokasyonlara sorunsuz ve hızlıca bağlamayı sağlar.

Sorunsuz veri aktarımının keyfini çıkarın

Bu çözüm, Müşteri Tarafı Cihazlar arasında dinamik tüneller yapılandırmanıza, uygulama trafiğini yönetmenize ve önceliklendirmenize, veri transferini optimize etmenize ve ağ işlevlerini verimli bir şekilde düzenlemenize olanak tanır.



Tek yönetim konsolu

Tüm ağını yönetin

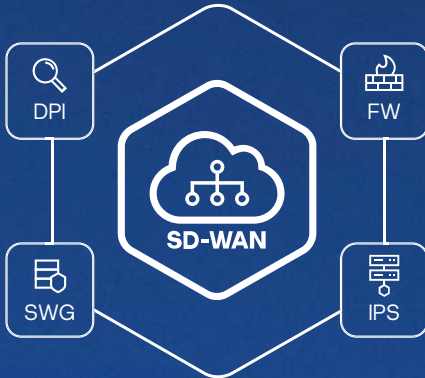
Birleştirilmiş bir web arayüzü, tüm ağı doğrudan orkestratörden veya Open Single Management Platform (OSMP) üzerinden yönetmenizi sağlar. CPE'yi yapılandırın, trafik filtreleme kuralları ve güvenlik ilkeleri oluşturun ve hizmetler için SLA'lar tanımlayın.

Altyapınızı oluşturun ve görselleştirin

Uygun grafik oluşturucu, yeni hizmetleri kolaylıkla entegre ederken ağ altyapınızı planlamanızı ve görselleştirmenizi sağlar – sanal ağ işlevlerini sürükleyip bırakmanız yeterlidir, ardından bu işlevler hemen başlatılabilir.

Bilgilendirici panolardan yararlanın

CPE, sanallaştırılmış işlevler ve fiziksel kaynaklar da dahil tüm altyapının durumu kontrolünüz altında ve parmaklarınızın ucunda.



Birleştirilmiş güvenlik

Tek güvenlik politikası

Bu çözüm VPN paylaşımı, merkezi cihaz yapılandırmaları, güvenlik politikaları ve akış kuralları kullanarak ve bunları WAN üzerinden dışarı aktararak şubeler için güvenlik sağlar.

Güvenlik araçlarını kolayca bağlayın

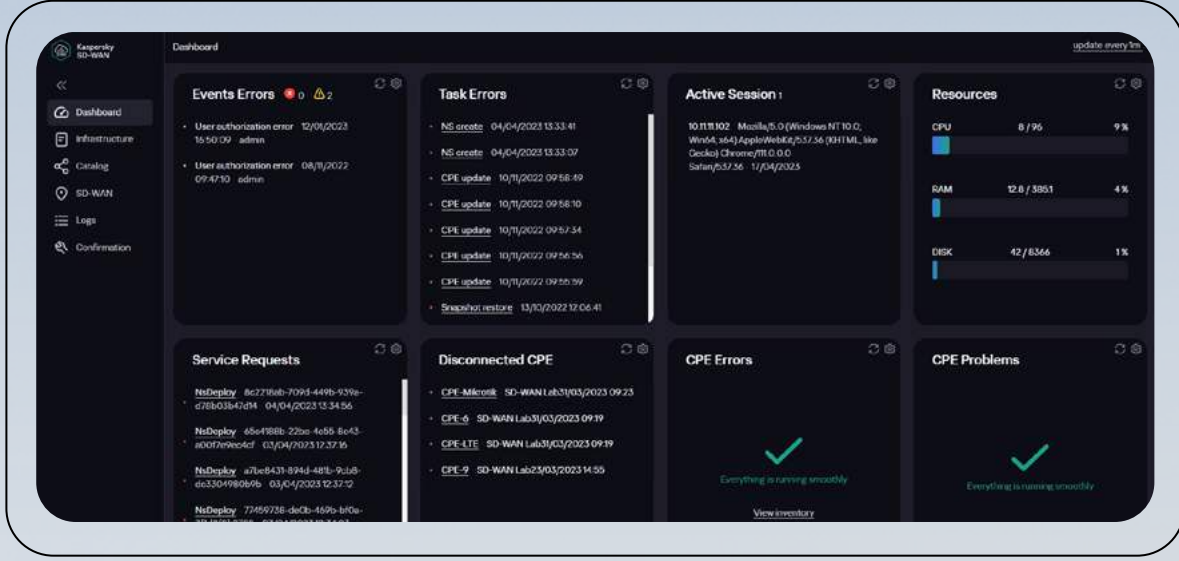
Ağ işlevleri sanallaştırması, güvenlik duvarları, güvenli web ağ geçitleri ve izinsiz giriş önleme sistemleri dahil olmak üzere trafik kontrolü ve güvenlik araçlarını otomatik olarak devreye almanıza olanak tanır.

Çok yönlü mimari

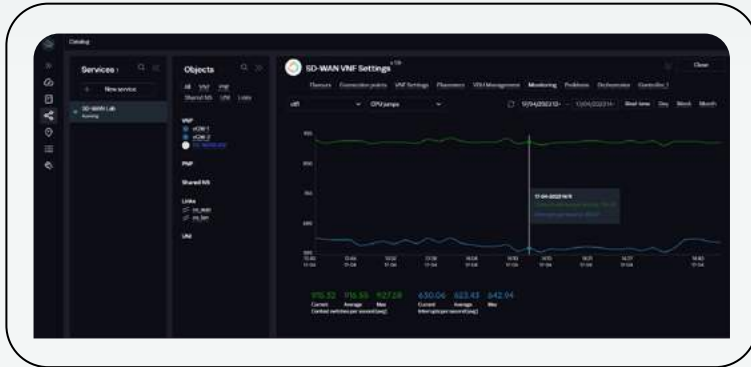
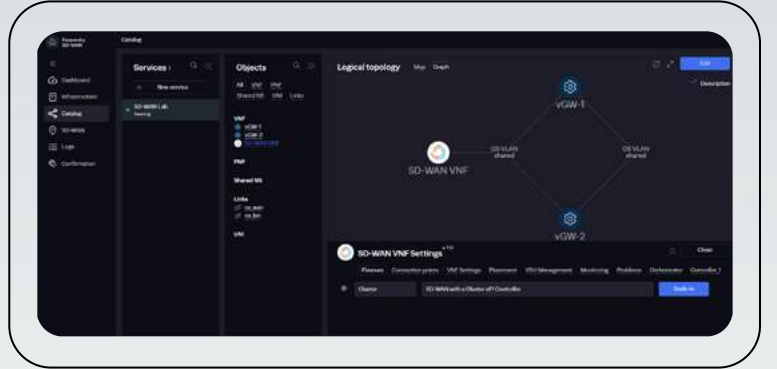
Mimarisindeki Sanal Ağ İşlevleri (VNF'ler) yöneticisi ve orkestratör sayesinde farklı tedarikçilerin güvenlik araçlarını kolayca entegre etmenizi sağlar.

Kullanışlı ve bilgilendirici web arayüzü

Çözüm ve ağ durumu hakkındaki temel bilgiler ana ekranda yer almaktadır



Kapsamlı özelliklere sahip kullanışlı
grafiksel hizmet zinciri oluşturucu



Çok çeşitli parametrelere dayalı sanal
ve sunucu kaynaklarının kullanımı

Çözümün kavramsal mimarisi

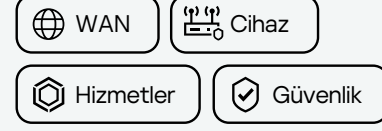
Güvenlik

Akış kontrolü ve güvenlik araçlarının otomatik uygulanması

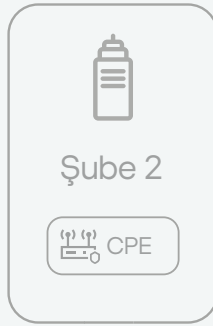
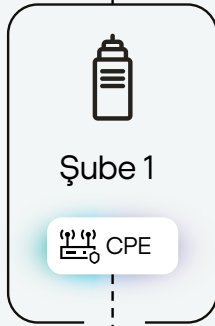
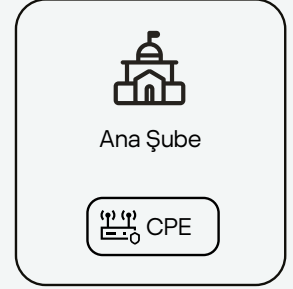
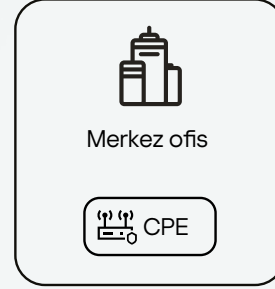
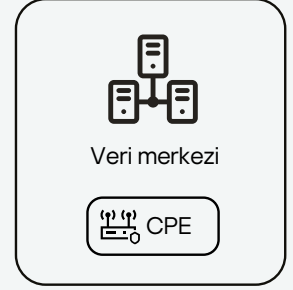
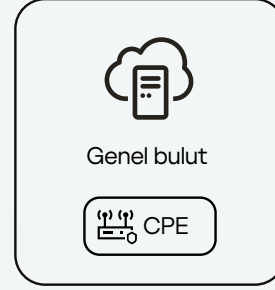


Yönetim

Yönetim için birleştirilmiş konsol:



Orkestratör ve denetleyiciyi devreye alma seçenekleri



...



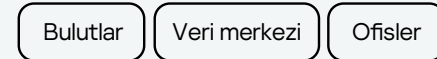
İletişim kanalları

İletişim kanallarını ve bu kanalların kombinasyonlarını seçme esnekliği



Erişim

Şunlara güvenli erişim:



Şirket kaynaklarına erişimi otomatik olarak ayarlayın

eDeploy yazılım ortamları (PaaS)

Kaspersky SD-WAN kademeleri ve kabiliyetleri

Kaspersky SD-WAN iki kademeye sahiptir: Standart ve Gelişmiş.

	Kabiliyetler	Standard	Advanced
 Bağlantı ve yönetim	10 Gb/s'ye kadar CPE çıkışı için destek	●	●
	Özel/genel buluttan veya şirket içinden yönetim	●	●
	Platform yönetiminin Open Single Management Platform (OSMP) ile entegrasyonu	●	●
	LAN ve WAN portları üzerinden kontrolör ile CPE bağlantısının organizasyonu	●	●
	Hub and Spoke, Full Mesh ve Partial Mesh topolojileri için destek	●	●
	Uygulamalar için SLA politikaları	●	●
	Dinamik yönlendirme (BGP, OSPF)	●	●
	VRF-Lite desteği	●	●
	Yerleşik DPI	●	●
	Durum Denetimli Koruma Duvarı	●	●
	NAT (PAT, SNAT, DNAT)	●	●
 SD-WAN Hizmetleri	El Değmeden Tedarik	●	●
	Gerçek zamanlı kanal kalite kontrolü	●	●
	Connectivity Fault Management (CFM)	●	●
	OpenFlow desteği	●	●
	Kanal optimizasyonu (FEC ve Paket Çoğaltma desteği)	●	●
	İlke Tabanlı Yönlendirme (PBR)	●	●
	P2P, P2M ve L2/L3 VPN hizmetleri için destek	●	●
	Dahili yüksek hızlı şifreleme desteği	●	●
 Sanal ağ işlevleri	Kaspersky ürünlerinin entegrasyonu için destek	●	●
	ETSI MANO		●
	Üçüncü taraf VNF'leri için destek		●
	Hizmet zinciri yaşam döngüsü yönetimi		●
	uCPE desteği		●
 Hizmetler	Çoklu gönderim desteği		●
	PIM desteği		●
	Çoklu kullanım desteği		●

Lisanslama

Bu çözüm CPE tarafından belirli iş hacmine göre lisanslanır. Çeşitli arayüzlere sahip Kaspersky SD-WAN Edge Service Router (KESR) serisinden önerilen modellerimizi seçebilirsiniz.



Güvenilir ağ ve güvenlik kabiliyetleri bir arada



Birleşik güvenlik taşıma omurgası

Kaspersky SD-WAN, güvenilir bir dağıtılmış ağın üzerine birleşik güvenlik inşa etmek için önemli bir adımdır. Kaspersky SD-WAN ile şimdi Secure Access Service Edge (SASE) oluşturmaya başlayabilirsiniz.

Kaspersky ekibi, siber güvenlik uzmanlığı konusunda eşsiz bir geçmişe sahiptir ve ürünlerimiz 700'den fazla bağımsız testte en etkili güvenlik çözümleri olarak değerlendirilmiştir. Ağ güvenliği çözümlerimizi aktif olarak geliştirirken, Secure Access Service Edge (SASE) kabiliyetleri ile müşterilerimizin korumasını artırmayı hedefliyoruz.

Kaspersky SD-WAN'ı bağlamak hızlı ve kolaydır

- 1 CPE'yi şubeye teslim edin
- 2 CPE'yi ağa bağlayın
- 3 Kullanıma hazır!

Güvenli yazılım geliştirme, Kaspersky SD-WAN'ın temelini oluşturur.

Kaspersky SD-WAN, diğer Kaspersky ürünleri gibi SSDLC (Güvenli Yazılım Geliştirme Yaşam Döngüsü) metodolojisine uygun olarak geliştirilmiştir.

Kaspersky Tehdit Araştırması, uzmanları ürünlerimizdeki güvenlik açıklarıyla ilgili riskleri azaltmakla uğraşan beş uzmanlık merkezimizden biridir.

Threat
Research



Daha fazla bilgi



Kaspersky SD-WAN

Daha fazla bilgi

www.kaspersky.com.tr

© 2025 AO Kaspersky Lab.
Tescilli ticari markalar ve hizmet markaları ilgili sahiplerinin
mülkiyetindedir.

#kaspersky
#geleceęiyakalayın