

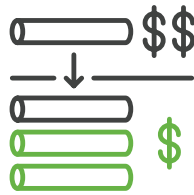
Cisco SD-WAN powered by Meraki

What is SD-WAN?

Software-defined wide area networking (SD-WAN) is a software-based approach for businesses to utilize and manage more than one external network connection such as MPLS, broadband, and fiber optic at a given location based on its performance.

With SD-WAN, network admins can define which WAN link an application should use, or set up rules for which link should be used based on its performance.

What can SD-WAN help achieve?



Reduce reliance on MPLS

In the past, organizations relied heavily on premium WAN links, such as MPLS, to ensure highly predictable and reliable connectivity. However, as bandwidth consumption continues to increase with more devices, increased usage of cloud applications, and video streaming, MPLS links are exceeding the capacity for which they were designed.

Low-cost links such as broadband and fiber have matured to now have the reliability and uptime to be viable options to provide additional bandwidth capacity or, in some instances, to replace MPLS altogether.

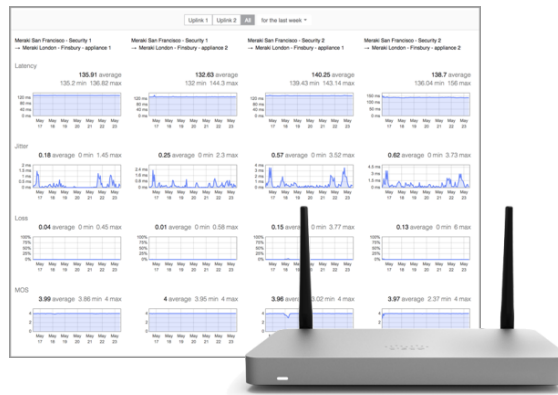


Maximize user experience in a multi-hosted environment

Applications are now hosted in multiple locations: the data center, IaaS, and SaaS providers—and are accessed in multiple ways, including direct Internet access. One of the key challenges to maximizing performance in such a multi-hosted environment is that organizations do not have ownership and hence direct management of public cloud environments, or the transit to them.

With more business-critical traffic becoming cloud-centric, use cases focused on intelligently maximizing SaaS application quality of experience (QoE) are emerging to be a vital expectation of SD-WAN.

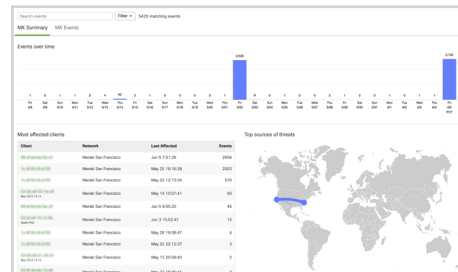
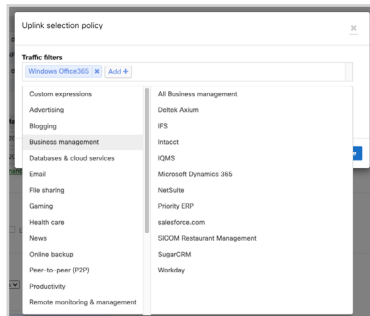
How does Cisco SD-WAN powered by Meraki work?



- Cisco SD-WAN powered by Meraki is delivered by the powerful Meraki MX appliances
- Two or more MX appliances can establish Auto VPN tunnels between devices (and locations) over any type of WAN link in three simple clicks
- The performance of all the VPN tunnels is monitored approximately every second for packet loss, jitter, latency, and MOS
- Advanced analytics also monitor key factors that influence how users experience business-critical resources to identify the root cause of any degradation in minutes
- Real-time performance telemetry is used to make autonomous decisions about which path should be used to satisfy the performance of critical cloud applications and VoIP



Why SD-WAN powered by Meraki?

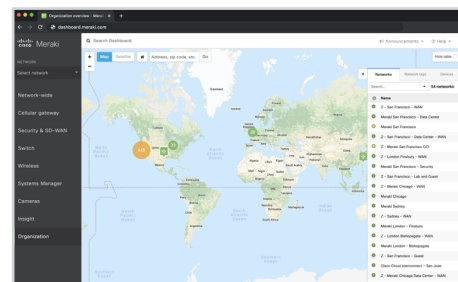
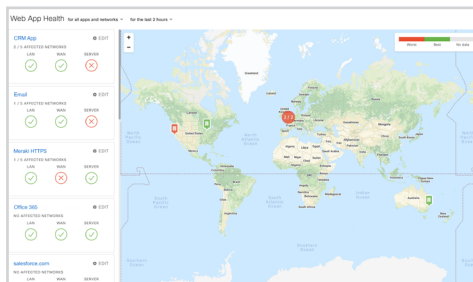


The simplest SD-WAN available

True zero-touch provisioning allows the quickest and simplest way for organizations to significantly reduce their total WAN costs and deliver the desired level of performance for VoIP and business critical cloud applications—no matter where they are hosted.

Natively secure SD-WAN

Natively integrated advanced security that includes next-gen layer-7 firewall, Cisco AMP with Threat Grid, Cisco SNORT IDS/IPS, cloud security with Cisco Umbrella SIG, and content filtering—to confidently allow direct Internet access.



Advanced analytics

Supreme visibility into key factors that influence how users experience business-critical resources to identify any degradation and its root cause in a matter of minutes.

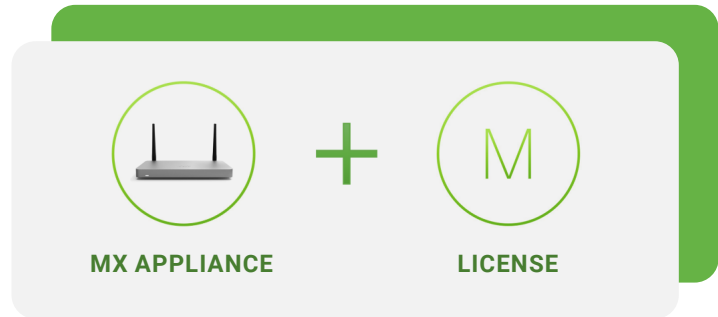
Unified management platform

Streamline IT operations with management of SD-WAN as well as wireless, switching, security, cellular, end-point management, and smart security cameras into a single intuitive and centralized platform.

- Web Application Health
- WAN Health
- VoIP Health

What's needed for Cisco SD-WAN powered by Meraki?

Cisco SD-WAN powered by Meraki is delivered by the MX appliances.



License options

The licensing structure for MX appliances is the same as that of any other Meraki device—a 1:1 ratio of devices to licenses. Pair your chosen MX appliance(s) with the relevant license for your use case.



Enterprise

Ideal for when seamless site-to-site VPN connectivity with a firewall is needed.

- Secure connectivity & basic security



Advanced Security

Ideal for organizations with sites also connecting to the Internet; unified threat management security is required.

- Secure connectivity & basic security
- Fully featured unified threat management



Secure SD-WAN Plus

Ideal for organizations reliant on apps served by SaaS, IaaS, or data-center locations.

- Secure connectivity & basic security
- Fully featured unified threat management
- Advanced analytics with ML
- Smart SaaS quality of experience
- Tag-based segmentation