

# Cisco Catalyst Software-Defined WAN (SD-WAN)

---

# Contents

Overview	3
Deploy and manage	4
Security	5
SD-WAN Analytics	9
Multicloud	13
Hybrid work	14
Positioning	15
Ordering and licensing	15
Multitenancy	17
Scalability	18
Programmability	18
Industry certifications	19
Services and resources	19

---

## Overview

**Q.** What is the Cisco Catalyst™ SD-WAN solution?

**A.** Traditional Wide-Area Networks (WANs), in which the majority of branch office traffic flows within an enterprise's intranet boundary, have been designed using Multiprotocol Label Switching (MPLS) for connectivity. However, new cloud applications, such as Microsoft 365 and Salesforce.com, and public cloud services, such as Amazon Web Services (AWS), Google Cloud, and Microsoft Azure, are changing traffic patterns. Today, the majority of enterprise traffic flows to public clouds and the internet. This change creates new requirements for security, application performance, cloud connectivity, WAN management, and operations.

Cisco Catalyst SD-WAN connects any user to any application, with integrated capabilities for multicloud, security, predictive operations, and enhanced network visibility – all on a Secure Access Service Edge (SASE)-enabled architecture. It helps ensure a predictable user experience for applications; optimizes software-as-a-service (SaaS), infrastructure-as-a-service (IaaS), and Platform-as-a-Service (PaaS) connections; and offers integrated security, either on-premises or in the cloud. Its analytics capabilities deliver the visibility and insights necessary to isolate and resolve issues promptly and deliver intelligent data analysis for planning and what-if scenarios. Above all, Cisco Catalyst SD-WAN is simple to operate. It offers:

- **Predictable application experience:** Increase user productivity by optimizing cloud and on-premises application performance with real-time analytics, visibility, and control.
- **Right security, right place:** Protect users, devices, and applications by deploying a cloud-delivered SASE or on-premises model, depending on the business requirements and compliance needs of the enterprise.
- **Simplicity at enterprise scale:** Centralize cloud management to make it easy to deploy SD-WAN and security while maintaining policy across thousands of sites.

**Q.** What problems does the Cisco Catalyst SD-WAN solution help solve?

**A.** The Cisco Catalyst SD-WAN solution solves many critical enterprise IT problems, including:

- Establishing a transport-independent WAN for lower cost and greater diversity.
- Meeting Service-Level Agreements (SLAs) for business-critical and real-time applications on-premises and in the cloud.
- Providing complete security from branch to SaaS and internet.
- Enabling secure multicloud transformation for enterprises.
- Providing centralized management, analytics, and policy across the global WAN.
- Providing multitenancy that lets you manage a multitude of customers and thousands of devices from a single dashboard, helping you simplify your operations.

---

**Q.** Who has deployed the Cisco Catalyst SD-WAN solution?

**A.** Cisco has one of the most widely deployed enterprise-grade SD-WAN solutions in the industry, with large deployments in many sectors in both enterprise and managed service provider infrastructures. Cisco boasts over 48,000 SD-WAN deployments, which is more than double the number of our closest competitor. The solution is deployed across Fortune 2000 companies and in 70% of Fortune 100 enterprises, with thousands of production sites in every major industry, including healthcare, manufacturing, retail, professional services, energy, oil and gas, insurance, finance, government, logistics, distribution, and more.

## Deploy and manage

**Q.** How do you manage and operate Cisco Catalyst SD-WAN?

**A.** Cisco Catalyst SD-WAN is a centrally managed, orchestrated, and operated solution with a cloud-hosted Cisco GUI management console and provisioning platform, SD-WAN controller, and orchestration layer at the heart of the solution.

**Cisco Catalyst SD-WAN controllers** are the centralized brain of the solution; they implement policies and connectivity between SD-WAN branches. The centralized policy engine in Cisco controllers provides policy constructs to manipulate routing information, access control, segmentation, extranets, and service chaining.

The entire solution is managed with **Cisco® vManage**. vManage lets IT managers and network operators centrally automate the configuration, management, and operation of the entire SD-WAN fabric, all in a highly visualized and intuitive user experience.

vManage offers an enhanced visualized experience that lets network operators quickly deploy, manage, and automate the network and devices across the entire SD-WAN fabric. vManage includes:

- A highly visualized and intuitive interface for easy consumption.
- Preconfigured templates that automate and expedite the deployment of most common use cases.
- Guided step-by-step configuration designed to intelligently expedite onboarding of new devices.
- A consistent user experience across Cisco solutions (Cisco DNA).

**Q.** How is Cisco Catalyst SD-WAN deployed at branch offices and data center networks or regional hubs?

**A.** At branch office and regional data center hub sites, Cisco Catalyst SD-WAN can be deployed and connected using either virtual or physical secure routers.

Enterprise customers and service providers can gain rich services such as WAN optimization and firewall or basic WAN connectivity for physical or virtual platforms across the branch, WAN, or cloud as follows:

### Physical

- **Branch:** Cisco IOS® XE and Viptela OS-based devices.
- **Branch:** Cisco Catalyst 8300 Series Edge Platforms and Cisco 1000, 1100, or 4000 Series Integrated Services Routers (ISRs).

- 
- **Branch, regional hub, or data center:** Cisco Catalyst 8500 Series Edge Platforms and Cisco ASR 1000 Series Aggregation Services Routers (ASRs)
  - **Virtual**
  - **SD-Branch:** Cisco 5000 Series Enterprise Network Compute System (ENCS) and Integrated Services Virtual Router (ISRv)
  - **Network hub, colocation facility, or data center:** Cisco Cloud Services Platform 5000, Catalyst 8000V Edge Software, and Cloud Services Router (CSR) 1000V Series

#### Public cloud (IaaS)

- Amazon Web Services
- Microsoft Azure
- Google Cloud

## Security

**Q.** What are the SD-WAN security features?

**A.** Cisco Catalyst SD-WAN builds on the SASE architecture. WAN security and features today must be distributed, cloud-based, flexible, and agile. Cisco Catalyst SD-WAN is the industry's first fully integrated SASE offering that combines best-in-class SD-WAN with the cloud-based Cisco Umbrella® or on-premises security portfolio. Both security architectures provide full protection for enterprises connecting to cloud and internet applications. These security features are:

- **Enterprise firewall:** Granular policy and control of thousands of applications.
- **Secure web gateway:** Full protection against all kinds of web-based attacks, including Secure Sockets Layer (SSL) inspection.
- **DNS layer security and URL filtering:** Stops threats at the earliest point, significantly reducing incidents.
- **Intrusion prevention system (IPS):** A built-in IPS within an on-premises enterprise firewall based on Snort® and powered by Cisco Talos®, one of the world's largest commercial threat intelligence teams.
- **Cloud access security broker (CASB):** Protection against account compromises, breaches, and other major risks in the cloud application ecosystem.
- **Malware protection:** An extended security feature across both on-premises and cloud security using Cisco Advanced Malware Protection (AMP).  
<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/ios-xe-17/security-book-xe/malware-protection.html> and Secure Malware Analytics to prevent and detect malicious files with sandboxing.

To learn more about SASE, see the [What Is SASE? page](#).

---

**Q.** How does Cisco Catalyst SD-WAN provide a zero-trust approach to security?

**A.** The integration between Cisco Catalyst SD-WAN and Cisco Identity Services Engine (ISE) provides a powerful set of security features that enables IT teams to employ zero-trust security functions for the traffic that goes through an SD-WAN fabric. Additionally, the use of SD-WAN Remote Access (SDRA) extends the application of zero-trust principles to remote users, providing enhanced security for organizations. The integration between Cisco Catalyst SD-WAN and ISE allows Cisco ISE to support the configuration of security posture policies in the SD-WAN fabric. Moreover, Cisco ISE shares the Security Group Tags (SGT) and session attributes with the Cisco Catalyst SD-WAN ecosystem, enabling IT teams to create identity groups and associate security policies in Cisco vManage to allow access by specific user groups to applications over the SD-WAN fabric, all the way to the edge. Additionally, Cisco ISE supports a periodic reassessment of device posture, allowing for changes in authorization and security policies at the SD-WAN edge.

**Q.** How is Cisco Catalyst SD-WAN integrated with Cisco Umbrella cloud security?

**A.** Cisco Catalyst SD-WAN provides complete integration with Cisco Umbrella cloud security. Using Cisco vManage, automatic registration and setup of tunnels to the Cisco Umbrella cloud can be executed within a few minutes, so that the enterprise is completely protected.

**Q.** Does Cisco Catalyst SD-WAN support Cisco Umbrella's multi-org integration?

**A.** Yes, Cisco Catalyst SD-WAN supports Cisco Umbrella's multi-org integration, allowing customers to easily manage multiple child orgs or regions from a single Umbrella dashboard. The ability to create customized security policies tailored to specific needs of different regions or organizational units allows customers to simplify the security management process, improve network security, and reduce the risk of security breaches.

**Q.** Does Cisco Catalyst SD-WAN support third-party integration with other cloud security vendors?

**A.** Yes, Cisco Catalyst SD-WAN supports third-party integration with widely popular cloud security providers such as Zscaler, Netskope, and Cloudflare. The integration with these vendors provides flexibility in the SASE journey to enterprises by providing a choice of networking and cloud security capabilities. Additionally, these integrations can help organizations leverage their existing investments in cloud security solutions by making it easier to integrate with Cisco SD-WAN.

**Q.** Does Cisco Catalyst SD-WAN support third-party integration with Security Information and Event Management (SIEM) providers?

**A.** Yes, Cisco Catalyst SD-WAN supports third-party integration with Splunk, which is a leading SIEM provider, to help users with a security dashboard. This dashboard captures vital data points and provides a holistic view of all security events in the network.

**Q.** Why does device and firmware security matter in Cisco Catalyst SD-WAN?

**A.** Firmware attacks on infrastructure have increased in frequency, severity, and costs, not just for public entities but also for enterprises and small businesses. These attacks are quiet, pervasive, and devastating, like many of the latest and most notable hacks. Cisco SD-WAN edge platforms and routers provide an extra layer of security via an advanced Trust Anchor, so that you can remotely activate, change, and control your SD-WAN platforms while remaining secure.

**Q.** Does the Cisco Catalyst SD-WAN solution support network segmentation, and what are the benefits?

**A.** Yes, the Cisco Catalyst SD-WAN solution supports network microsegmentation and identity-based policy management across Cisco Software-Defined Access (SD-Access) and non-SD-Access branches. Microsegmentation provides secure logical isolation on the SD-WAN network, where each segment is defined as a separate VPN and controlled centrally by access control policies. Some of the benefits of segmentation include:

- Security is increased by isolating your network from outside attackers and creating secure separation within multiple application segments.
- Acquisitions can be integrated into the parent network and yet kept separate. Policies control what applications the acquired company can access.
- Guest Wi-Fi can be maintained on a separate, low-priority segment and offloaded onto the internet at the closest exit point.
- Business partners can each be defined in a separate segment or in a collective business-partner network segment. Policies control business partners' access to data center applications.
- A single pane of glass helps organizations to avoid complex configurations and frequent policy changes that lead to uneven user experience, thereby increasing overall network efficiency and reliability.

For more information, see [Cisco SD-WAN Segmentation Configuration Guide: Segmentation \(VPN\) Overview](#).

**Q.** What are the SD-WAN security capabilities, and which platforms support SD-WAN security?

**A.** Cisco Catalyst SD-WAN security capabilities include an application-aware enterprise firewall, intrusion prevention, DNS layer enforcement (Cisco Umbrella), and URL filtering. Cisco Catalyst SD-WAN reduces complexity by having a single management interface (vManage) for both the network and security.

Platform support for SD-WAN security is shown in the following table.

**Table 1.** SD-WAN security highlights

Platform	Enterprise firewall	Enterprise firewall application awareness	IPS	URL filtering	AMP and Secure Malware Analytics	Full cloud security with Cisco Umbrella
<b>1000 Series ISRs</b>	Yes	Deep Packet Inspection (DPI) using Qosmos	X	X	X	Yes
<b>CSR 1000V</b>	Yes	Yes	Yes	Yes	Yes	Yes
<b>Catalyst 8000V Edge Software</b>	Yes	Yes	Yes	Yes	Yes	Yes
<b>ISRv, 5000 Series ENCS</b>	Yes	Yes	Yes	Yes	Yes	Yes
<b>Catalyst 8300 Series</b>	Yes	Yes	Yes	Yes	Yes	Yes
<b>4000 Series ISRs</b>	Yes	Yes	Yes	Yes	Yes	Yes

Platform	Enterprise firewall	Enterprise firewall application awareness	IPS	URL filtering	AMP and Secure Malware Analytics	Full cloud security with Cisco Umbrella
1111X-8P ISR	Yes	Yes	Yes	Yes	Yes	Yes
1111-4P, 1111-8P, 1116-4P, and 1117-4P ISRs (1000 Series ISRs)	Yes	Yes	X	X	X	Yes
Catalyst 8500 Series	Yes	Yes	X	X	X	Yes
ASR 1000 Series	Yes	Yes	X	X	X	Yes

- Q.** Can the Cisco Catalyst SD-WAN solution provide insight into threats in encrypted traffic without the need for decryption?
- A.** Encrypted Traffic Analytics (ETA) is not currently supported for the Cisco Catalyst SD-WAN solution but is planned to be introduced in the future. For more information on ETA, see <https://www.cisco.com/c/en/us/solutions/enterprise-networks/enterprise-network-security/eta.html>.
- Q.** Does Cisco Catalyst SD-WAN support identity firewall capabilities?
- A.** Yes, vManage integration with the Cisco ISE applies policies based on identity within the SD-WAN network. ISE interfaces with external Active Directory (AD) to provide user identity mapping. It helps customers to configure access rules and security policies based on user names and user group names and classification of flows and enhances SD-WAN policies with identity information on edge routers so that customer intent can be addressed by employee identity and/or role across SD-WAN. It also helps customers address the security limitations associated with IP addresses/subnets, ports, Fully Qualified Domain Names (FQDN), geo locations, protocols, and applications and enables more fine-grained control with security policies based on user identity and user groups.
- Q.** Does Cisco Catalyst SD-WAN offer any insights to the SecOps team regarding security events?
- A.** Yes, Cisco Catalyst SD-WAN provides insights on security events to the SecOps team. In addition to a NetOps persona, a new SecOps persona is available in the Cisco vManage controller. When the SecOps persona logs in to the controller, they are presented with a security-focused dashboard and have access to management privileges. This allows the security administrator to quickly gain a comprehensive understanding of the security health of the network, including insights into security events. Additionally, the vManage controller includes a security-focused SecOps dashboard that provides a centralized view of network security events and actionable threat data for Security Operations Center (SOC) teams.



---

## SD-WAN Analytics

**Q.** How does a lack of application visibility impact overall IT operations?

**A.** Applications and users are more distributed than ever, and the internet has become the new enterprise WAN. As SD-WAN has transformed to connect users across multicloud, branch, data centers, and a hybrid workforce, enterprises and other organizations are constantly challenged to deliver reliable connectivity, application performance, and security over networks and services they don't own or directly control.

IT and network teams often carry the burden of proving the network innocent when something goes wrong. Application issues might manifest as network issues. Service disruptions can lead to endless finger-pointing. The resulting cycles spent pinpointing the source of issues can lead to prolonged service interruptions that ultimately damage the revenue and reputation of the business. To deliver transformation, IT leaders need a network analytics solution that provides visibility, predictivity, and automation to help them simplify network operations over such a dynamic environment.

**Q.** What is Cisco Catalyst SD-WAN Analytics?

**A.** Cisco Catalyst SD-WAN Analytics simplifies network operations by providing granular network insights, predictivity, and automation that not only heighten network integrity but also deliver an optimal application experience. By liberating IT and network teams from complex network operations, Cisco SD-WAN empowers IT and network teams to maximize productivity and improve operational efficiency and resiliency, ultimately accelerating digital transformation and innovation.

Cisco Catalyst SD-WAN Analytics consists of Cisco vAnalytics, Predictive Path Recommendations, and Cisco ThousandEyes®.

**Q.** What is Cisco vAnalytics?

**A.** Cisco vAnalytics aggregates a large volume of telemetry data and correlates application performance with underlying networks for operational insights in a highly visualized and simplified manner. vAnalytics enhances network visibility, establishes historical benchmarks, and expedites root-cause isolation, ultimately enabling enterprises to take the necessary corrective actions and gain total control of the user experience.

For more information, see <https://www.cisco.com/c/en/us/solutions/enterprise-networks/sd-wan-analytics/index.html>

**Q.** Can Cisco vAnalytics provide enhanced visibility and insights for Microsoft 365 applications?

**A.** Yes, Cisco vAnalytics provides enhanced visibility and insights for Microsoft 365-informed network routing by providing visibility into network Quality of Experience (QoE) metrics and Microsoft telemetry metrics for each available path. Microsoft 365 path analytics provide visibility into which path is being used by Microsoft 365 traffic over a given period, enabling network operators to easily visualize the best path. This helps in monitoring the traffic and application experience and provides insights to make troubleshooting easier.

---

**Q.** Can Cisco vAnalytics extend visibility into Webex by Cisco?

**A.** Cisco vAnalytics, integrated with Webex telemetry, provides enhanced visibility with insights into application and network performance metrics. With the Webex app providing feedback via telemetry, customers can visualize the app performance metrics such as loss, latency, jitter, resolution height, media-bitrate, framerate, and much more via the Webex 360 panel within the Cisco vAnalytics dashboard. Webex telemetry also provides insights into application perspective via network Key Performance Indicators (KPIs) such as loss, latency, etc., offering a holistic view of network and application health. This feature also empowers IT teams and network administrators of organizations to proactively identify and resolve network or application problems across their global offices, for an improved user experience.

**Q.** How is vAnalytics activated?

**A.** Cisco vAnalytics can be activated from vManage or the [Cisco Catalyst SD-WAN Self-Service Portal](#). Please refer to the [Cisco vAnalytics user guide](#) for details.

**Q.** What is Predictive Path Recommendations?

**A.** Predictive Path Recommendations (PPR), powered by ThousandEyes WAN Insights, an integral component of Cisco Predictive Networks, delivers a predictive network solution, enabling Cisco Catalyst SD-WAN customers to proactively improve the application experience for users. Leveraging advanced algorithms and predictive models, PPR determines the performance and policy compliance of the paths carrying the site application traffic. When performance is below historical benchmarks or SLAs, PPR can make recommendations and automatically implement corrective actions – before users are impacted.

**Q.** How is Predictive Path Recommendations activated?

**A.** PPR is included in Cisco DNA Advantage. It can be activated from vManage or the [Cisco Catalyst SD-WAN Self-Service Portal](#). Please refer to the [Cisco vAnalytics user guide](#) for details.

**Q.** What is Cisco ThousandEyes?

**A.** ThousandEyes enables enterprises that are increasingly dependent on internet, cloud, and SaaS to see, understand, and improve digital experiences for customers, employees, and users. Its end-to-end visibility from any user to any application over any network enables enterprises to quickly pinpoint the source of issues, get to resolution faster, and measure and manage the performance of what matters.

ThousandEyes collects multilayer telemetry data from vantage points distributed throughout the internet, as well as in enterprise data centers and cloud, branch, and campus environments, providing detailed metrics on conditions between those vantage points and applications and services distributed throughout the globe. The result is insight into the application experience and underlying dependency, whether network, service, or application related.

For more information, see <https://www.thousandeyes.com>.

---

**Q.** How is Cisco Catalyst SD-WAN integrated with ThousandEyes?

**A.** Cisco Catalyst SD-WAN is the only SD-WAN solution with turnkey ThousandEyes vantage points. The solution supports eligible routers from the Cisco Catalyst 8200, 8300, and 8500 Series Edge Platforms, Cisco 4000 and 1000 Series ISRs, and ASR 1000 Series. Existing customers can expedite the deployment of ThousandEyes agents with the vManage integration and enable faster time to value for their IT operators.

For more information, see the [Cisco Catalyst SD-WAN with Cisco ThousandEyes integration](#) video.

**Q.** How is ThousandEyes ordered?

**A.** Customers can leverage an existing ThousandEyes subscription with eligible Cisco Catalyst 8200, 8300, and 8500 Series Edge Platforms and Cisco 4000 and 1000 Series ISRs, as well as Cisco ASR 1000 Series routers.

- Existing ThousandEyes customers can use their available ThousandEyes license and units toward new tests.
- New ThousandEyes customers will need to purchase a ThousandEyes license to activate the ThousandEyes agents.

**Q.** What is the difference between ThousandEyes and Cisco vAnalytics?

**A.** Cisco vAnalytics aggregates a large volume of telemetry data and correlates application performance with underlying networks for operational insights, in a highly visualized and simplified manner. ThousandEyes enables enhanced visibility beyond the traditional SD-WAN fabric into the internet, cloud, and SaaS to deliver an optimal application experience.

**Q.** When do I deploy Predictive Path Recommendations? How about ThousandEyes WAN Insights?

**A.** PPR and ThousandEyes WAN Insights are interdependent applications. WAN Insights offers a predictive engine, whereas PPR provides critical telemetry and closed-loop automation. We recommend that existing ThousandEyes users leverage WAN Insights from their existing ThousandEyes dashboard, and that Cisco Catalyst SD-WAN users deploy PPR within their existing vAnalytics environment.

**Q.** How does Cisco Catalyst SD-WAN Analytics deliver greater application visibility?

**A.** Cisco Catalyst SD-WAN Analytics enables greater visibility for IT and network operators to drive optimal digital experience across the internet, cloud, and SaaS. With this solution, you can:

- Gain enhanced visibility into the network underlay, including detailed path and performance metrics.
- Measure and proactively monitor SD-WAN overlay performance and routing policy validation.
- Determine the reachability and performance of SaaS and internally owned applications.
- Establish network and application performance baselines across global regions before, during, and after deployment of SD-WAN to mitigate risk and establish and validate KPIs.
- Predict probabilities of traffic disruption for different applications and use these forecasts to provide recommended network paths, thereby preventing user-impacting issues from occurring, eliminating the need for reactive network changes, and subsequently reducing the impact on user experience.
- Correlate raw telemetry sources, establish historical benchmarks, and provide operational insights, thereby transforming network operations from a reactive model to a highly predictive one.

- 
- Offer a seamless Microsoft 365 and Webex user experience via telemetry, path optimization, and policy automation.
  - Deploy highly visualized graphic capabilities that simplify analytics for an improved user experience.
  - Offer your CIO, CTO, and COO visual representation and analysis reports for offline review.

**Q.** What are the benefits of Cisco Catalyst SD-WAN Analytics?

**A.** With Cisco Catalyst SD-WAN Analytics, IT managers can rapidly pinpoint the root cause of application and network disruptions, provide actionable insights, and accelerate resolution time.

- **Optimize efficiency:** Correlate raw telemetry sources, establish historical benchmarks, and provide operational insights, thereby transforming network operations from a reactive model to a highly predictive one.
- **Optimize user experience:** Provide the unified application experience your end users have come to expect, regardless of their location and associated network environment.
- **Optimize resiliency:** Monitor network and application performance proactively, while validating implemented policies with business requirements to avoid performance issues that could impact users.
- **Optimize operational sustainability:** Establish a perpetual optimization cycle that achieves overall CapEx and OpEx efficiency. Predictive analytics enhance resource planning and network engineering that enable organizations to forecast optimal capacity, thereby driving CapEx efficiency. OpEx efficiency is achieved by proactively preventing user-impacting issues, automating resolution, and reducing overall troubleshooting cycles.
- **Optimize productivity:** Create a proactive engagement model that allows network conditions that may otherwise have gone unnoticed to be addressed before they reach a noticeable level. A proactive operating model will ultimately free up resources and time that can be shifted to higher-level strategic and innovation priorities.
- **Optimize operations:** Deliver strategic business outcomes to enterprise and service providers. Workforce challenges in the IT sector are not new, with ongoing difficulties in finding the right talent to keep up with attrition and growth. Skill gaps grow greater each year as employers chase a smaller pool of highly skilled workers with expertise in cloud-native platforms, networking engineering, and security. Enhanced visibility, automation, and prediction can fill the gaps by standardizing operations and executing routine operational activities on a proactive basis.

---

## Multicloud

**Q.** Can the Cisco Catalyst SD-WAN solution provide automated connectivity and optimization for IaaS and SaaS platforms such as AWS, Microsoft Azure and Microsoft 365, Google Cloud, Salesforce.com, Webex, etc.?

**A.** The Cisco Catalyst SD-WAN fabric connects users at the branch through the internet, through interconnect providers, or even via colocation environments to applications in the cloud in a seamless, secure, and automated fashion. Cisco delivers this comprehensive capability for IaaS and SaaS applications with Cisco SD-WAN Cloud OnRamp, which is currently available with Cisco IOS XE SD-WAN or Viptela OS platform SD-WAN solutions.

With Cloud OnRamp, the Cisco Catalyst SD-WAN fabric continuously measures the performance of a designated application through all permissible paths from a branch (MPLS, internet, 4G LTE, etc.). The SD-WAN fabric automatically makes real-time decisions to choose the best-performing path between the end users at a remote branch and the cloud application. Enterprises and service providers have the flexibility to deploy this capability in multiple ways and according to business needs and security requirements.

For more information, see <https://www.cisco.com/c/en/us/solutions/enterprise-networks/sd-wan/cloud-onramp.html>.

**Q.** Does Cisco Catalyst SD-WAN support Software-Defined Cloud Interconnect (SDCI) or middle-mile connectivity?

**A.** Yes, with Cisco Catalyst SD-WAN you can have fast, secure, and private network connectivity between your branches, data center, and the world's leading cloud providers, from anywhere. Cisco Catalyst SD-WAN's middle-mile network optimization solutions offer anywhere to everywhere connectivity within minutes. Through centralized control with a choice of middle-mile providers, Cisco Catalyst SD-WAN can connect users and workloads from site to site, site to cloud, or cloud to cloud. Integrating a middle-mile provider's private backbone with Cisco Catalyst SD-WAN allows you to strengthen your security posture and maximize protection for users with complete end-to-end encryption and segmentation. Using the vManage controller, you get full network stack automation and visibility to provision and orchestrate the entire network – simplifying your day-to-day operations.

**Q.** Can the Cisco Catalyst SD-WAN solution provide end-to-end encryption of traffic traversing a third-party backbone?

**A.** Yes, Cisco SD-WAN Cloud Interconnect offers end-to-end encryption of traffic from the branch to the cloud through the middle-mile backbones of AWS, Google Cloud, Microsoft Azure, Megaport, or Equinix. Cisco extends the SD-WAN fabric over the private underlay all the way into the cloud service provider by hosting virtual SD-WAN routers in transit Virtual Private Clouds (VPCs) and Virtual networks (VNETs).

This not only allows for end-to-end encryption for the branch-to-cloud traffic but also ensures that traffic is automatically steered to alternate paths for site-to-cloud traffic whenever the primary underlay path is unavailable.

---

## Hybrid work

**Q.** Does Cisco Catalyst SD-WAN support a remote workforce?

**A.** The Cisco Remote Workforce Routing solution extends uniform enterprise SD-WAN to a home and remote workforce. Extensive cloud integration delivers a consistent and optimal application experience. The cloud-delivered SASE architecture provides unified security and compliance. Centralized management automates deployment, configuration, and troubleshooting in an agile and scalable manner. The Cisco Remote Workforce Routing solution consists of the following flexible hardware and software solutions:

- **Cisco 1131 ISR:** The ability to connect users reliably and securely across multicloud, branch, data center, and hybrid workforce has become a critical success factor to any organization. The 1131 ISR is the next iteration of ISRs, optimized for distributed small branches and a remote workforce, with built-in Wi-Fi 6 and 5G support for enhanced SD-WAN connectivity.
- **Cisco Catalyst SD-WAN Remote Access (SD-WAN RA):** Integrates remote access functionality into the SD-WAN fabric, thereby delivering all the benefits of Cisco Catalyst SD-WAN to the remote workforce. Remote workers can simply leverage existing remote access clients (including Cisco AnyConnect®, Windows, Apple OS native clients, and hardware-based routers) to access the nearest Cisco Catalyst SD-WAN edge device, regardless of their location and devices.
- **Cisco Catalyst Wireless Gateway CG113 Series:** This simple-to-deploy wireless router is designed to empower the remote workforce to collaborate like never before. Flexible Wi-Fi 6 and cellular failover deliver a consistent application experience, with enterprise Wi-Fi connectivity and security extended to the remote workforce. A centralized dashboard automates deployment and management in an agile manner. A small and silent form factor accelerates the transition to a hybrid workforce where and when it is needed.

**Q.** What are the key benefits and features of these routing solutions?

**A.** These solutions:

- Provide a consistent and optimized application experience with seamless connectivity to cloud and SaaS applications.
- Automate the deployment, configuration, and management of hybrid work routing solutions with Cisco vManage.
- Integrate a cloud-delivered SASE architecture for unified security policy and compliance across a hybrid workforce.
- Enable adoption of scalable hardware or software endpoint options that accelerate the transition to hybrid work where and when they are needed, in a simple and agile manner.
- Can leverage existing branch infrastructure, thereby lowering overall TCO while extending enterprise-grade SD-WAN in a flexible and distributed manner.
- Provide end-to-end micro- and macrosegmentation.
- Are based on a highly scalable and distributed architecture, eliminating single points of failure in the network.

---

## Positioning

**Q.** What is the difference between Cisco Catalyst SD-WAN and Cisco Meraki® SD-WAN?

**A.** Cisco Catalyst SD-WAN can help your business no matter its size with a variety of deployment options. For lean IT operations, Cisco Catalyst SD-WAN powered by Meraki is preferred, and for full-featured, sophisticated deployments, Cisco Catalyst SD-WAN powered by Viptela is preferred.

- **Lean IT operations:** Deploy Cisco Catalyst SD-WAN powered by the Meraki MX unified threat management hardware, and enjoy a unified, secure SD-WAN for businesses with lean IT teams.
- **Branches and campuses:** With both physical and virtual options, you can deploy Cisco SD-WAN on the Catalyst 8000V, CSR 1000V, Catalyst 8300 Series, 1000 and 4000 Series ISRs, or with Network Functions Virtualization (NFV) using Cisco SD-Branch with the ISRv on the 5000 Series ENCS and Cisco UCS® E-Series platforms.
- **Headquarters, data center, and colocation:** With physical or virtual options, deploy Cisco Catalyst SD-WAN on the Catalyst 8500 Series, the ASR 1000 Series, or with NFV and network hub solutions on the Cisco Cloud Services Platform 5000.

## Ordering and licensing

**Q.** How is the Cisco Catalyst SD-WAN solution ordered?

**A.** Please consult the [Cisco DNA Software for SD-WAN and Routing Ordering Guide](#).

**Q.** How is the Cisco Catalyst SD-WAN solution licensed?

**A.** The Cisco Catalyst SD-WAN solution license is called Cisco DNA Software for SD-WAN and Routing. Three levels of subscription licenses are available: Cisco DNA Essentials, Cisco DNA Advantage, and Cisco DNA Premier. Similar to the subscription offers for switching and wireless, these are nested SKUs and represent good, better, and best offers. For more information, see the [Cisco DNA Software for SD-WAN and Routing page](#).

**Q.** Is a Cisco DNA license mandatory?

**A.** Cisco DNA Software is mandatory for the Catalyst 8000 Edge Platforms Family at the initial time of purchase of the hardware. An active Cisco DNA Software stack entitlement is mandatory for any SD-WAN deployment, regardless of device or platform.

For a list of SD-WAN-capable Cisco IOS XE platforms, see the [SD-WAN Release Notes](#).

**Q.** What are the Cisco DNA subscription offers?

**A.** There are three Cisco DNA SD-WAN and Routing subscription offers to choose from. A subscription can be purchased either as an individual transaction or as an enrollment in a [Cisco Enterprise Agreement](#). Subscription licenses can be purchased for a 3- or 5-year term. Cisco DNA Advantage is also available in a 7-year term. Software licenses are portable across the cloud and premises, are easy to upgrade across tiers, and include Software Support Service (SWSS) for the Cisco DNA Software stack.

The following table describes the components in each Cisco DNA Software for SD-WAN and Routing subscription license.

**Table 2.** Licensing options

Component	Description
<p><b>Cisco DNA Premier for SD-WAN and Routing</b></p>	<p>Cisco DNA Premier for SD-WAN and Routing is an SD-WAN subscription package with advanced SD-WAN security to mitigate the most sophisticated threats to your business.</p> <p>This package contains all components from Cisco DNA Essentials for SD-WAN and Routing and Cisco DNA Advantage for SD-WAN and Routing and includes the following features:</p> <ul style="list-style-type: none"> <li>• Cisco Umbrella® SIG Essentials</li> <li>• Cisco Secure Malware Analytics with Sandboxing</li> </ul>
<p><b>Cisco DNA Advantage for SD-WAN and Routing</b></p>	<p>Cisco DNA Advantage for SD-WAN and Routing delivers flexible connectivity, enhanced security for feature-rich and valued branch deployment models, and a robust application experience.</p> <p>This package includes all components from Cisco DNA Essentials for SD-WAN and Routing as well as the following features:</p> <ul style="list-style-type: none"> <li>• Unlimited segmentation</li> <li>• vAnalytics</li> <li>• Predictive Path Recommendations (PPR), powered by ThousandEyes WAN Insights</li> <li>• Advanced Cloud OnRamp for Multicloud and SaaS (all applications and telemetry)</li> <li>• AppQoE</li> <li>• Automated service switching for Cisco and third-party Virtual Network Functions (VNFs)</li> </ul>
<p><b>Cisco DNA Essentials for SD-WAN and Routing</b></p>	<p>Cisco DNA Essentials for SD-WAN and Routing provides centralized and secure SD-WAN management and security protection for the cost-conscious customer.</p> <p>This package enables the following SD-WAN and traditional WAN features:</p> <ul style="list-style-type: none"> <li>• Limited segmentation (four user VPNs, one management VPN)</li> <li>• vManage for centralized management (cloud or on-premises)</li> <li>• Flexible topology (hub and spoke, partial mesh, full mesh)</li> <li>• Application-based policies (including application-aware routing policies)</li> <li>• Essential SD-WAN security services, including Layer 3/Layer 4 application-aware firewall, Snort IPS/IDS with Talos signature updates, URL filtering, Cisco Secure Endpoint (formerly AMP for Endpoints), Cisco Umbrella cloud-app discovery, SD-WAN Application Intelligence Engine (SAIE)</li> <li>• Essential cloud networking, including Multicloud: Google Cloud Platform (GCP), Amazon Web Services (AWS), Azure, SaaS: All applications</li> <li>• DNS monitoring and connector for Cisco Umbrella</li> <li>• Basic path optimization capabilities, including Forward Error Correction (FEC)</li> <li>• Dynamic routing protocols (Open Shortest Path First [OSPF]/Border Gateway Protocol [BGP])</li> </ul>

Please consult the [Cisco DNA for SD-WAN and Routing Feature Matrix](#) for the most current product information.

**Q.** What is included in the Cisco DNA for SD-WAN and Routing software license?

**A.** Cisco DNA for SD-WAN and Routing subscriptions include a perpetual network stack license and a term-based Cisco DNA software stack license. After the subscription term expires, customers will retain the network stack entitlement; however, for any SD-WAN deployment, an active Cisco DNA software stack entitlement is mandatory.



---

**Q.** What are the entitlements of the perpetual network stack?

**A.** The perpetual network stack provides entitlements for non-SD-WAN features (autonomous mode). For a complete listing of network stack entitlements, see the [Cisco DNA Software SD-WAN and Routing Matrix](#).

**Q.** What are the entitlements of the Cisco DNA subscription software stack?

**A.** The Cisco DNA subscription software stack provides entitlements for SD-WAN features (controller mode) including cloud-hosted vManage, vSmart, and vBond devices. For a complete listing of network stack entitlements, see the [Cisco DNA Software SD-WAN and Routing Matrices page](#).

**Q.** Are the Cisco DNA subscription licenses portable and able to be moved to another hardware platform?

**A.** Yes, the Cisco DNA software licenses can be moved across routing platforms, including 1000 and 4000 Series ISRs, Catalyst 8300 and 8500 Series, ASR 1000 Series, 5000 Series ENCS, and Cisco vEdge routers. With software portability you have investment protection for your licenses, regardless of which Cisco routing platform you choose now or upgrade to in the future. For more information, see the [Software License Portability Policy](#).

## Multitenancy

**Q.** Does the Cisco Catalyst SD-WAN solution support multitenancy?

**A.** Yes, Cisco Catalyst SD-WAN multitenant controllers let you manage a multitude of customers and thousands of devices from a single pane of glass, helping you simplify your operations. You can save on CapEx by making more efficient use of your platform investment by sharing the management, control, and orchestration plane across multiple customers. This enables you to achieve potential savings of greater than 85% (when compared to a single-tenancy model) by reducing servers, rack space, and cables for deploying controllers.

With Cisco Catalyst SD-WAN multitenant controllers, control, visualization, and access to the overall configuration of each tenant are enabled using "provider" privileges. Each tenant has their own dashboard and can be assigned "tenant" privileges to build network policies specific to their organization's requirements.

For more information, view the [configuration guide](#).

---

## Scalability

**Q.** Can we divide the architecture of a single Cisco Catalyst SD-WAN overlay network to increase the scalability?

**A.** Yes, Cisco Catalyst SD-WAN Multi-Region Fabric (also called Hierarchical SD-WAN) provides the ability to easily divide a single Cisco Catalyst SD-WAN overlay network into multiple regions and a central core-region network for managing interregional traffic. The SD-WAN Multi-Region Fabric architecture enables you to use different traffic transport service providers for each region, and for the central core-region network, to optimize cost and traffic performance. It also simplifies traffic configuration for some scenarios and provides a robust, adaptive topology that can help prevent routing failures in specific network scenarios. SD-WAN Multi-Region Fabric is a core enabler for WAN architectures involving a middle-mile WAN. It's a foundational capability that underpins our journey to multicloud and SDCI. SD-WAN Multi-Region Fabric offers managed service providers and global enterprises the ability to enhance, scale up, and more importantly, simplify Cisco Catalyst SD-WAN fabric across regions.

For more information, view the [configuration guide](#).

**Q.** Does the SD-WAN Cloud OnRamp capability of Cisco Catalyst SD-WAN support the Multi-Region Fabric architecture?

**A.** Yes, Cloud OnRamp supports the Multi-Region Fabric architecture. The Multi-Region Fabric architecture can be used to deploy SDCI-related Cisco Catalyst SD-WAN infrastructure by using the CoR Multicloud Interconnect Gateway workflows on vManage. The capabilities within the Multi-Region Fabric architecture improve the user experience of the IT team by enabling simplified control policy configuration and automatic resolution of routing loop and blackhole scenarios, and by providing the ability to assign regions and roles to SD-WAN edges deployed within the SDCI infrastructure.

**Q.** Can the Cisco Catalyst SD-WAN Multi-Region Fabric be segmented into multiple subregions?

**A.** Yes, the Cisco Catalyst SD-WAN Multi-Region Fabric supports dividing a given access region into multiple subregions and sharing Border Routers (BRs) between these subregions, allowing for flexible BR redundancy and failover-centric network designs. The introduction of subregions enables users to create subdomains of full-mesh connectivity between branch sites within a region, such that devices in the same subregion communicate directly.

## Programmability

**Q.** Is Cisco Catalyst SD-WAN programmable, and does it support APIs?

**A.** Yes, the Cisco Catalyst SD-WAN solution is open and programmable, with open APIs. Cisco Catalyst SD-WAN provides service providers and partners the opportunity to create new and unique services, including operational and business support systems. With Cisco Catalyst SD-WAN you can access the available Representational State Transfer (REST) APIs, create API calls, obtain device and interface information using code, pass parameters and write applications, and work on innovative solutions.

---

As part of the SD-WAN developer resources and learning content, there are two additional resources that are great value-added services for developers:

- **DevNet Ecosystem Exchange** makes it easy to find and share an application or solution built for Cisco platforms. Business leaders and developers alike can use this online portal to discover partner solutions that span all Cisco platforms and products. Currently, this central repository for developers contains over 1300 solutions.
- **DevNet Code Exchange** gives developers a place to access and share software to quickly build next-generation applications and workflow integrations. It offers a curated list of sample code, adapters, tools, and Software Development Kits (SDKs) available on GitHub and written by Cisco and the DevNet community. Code Exchange spans Cisco's entire portfolio and is organized according to Cisco platform and product areas.

For more information, see the SD-WAN Developer Center at <https://developer.cisco.com/sdwan>.

## Industry certifications

**Q.** What industry certifications does Cisco Catalyst SD-WAN have?

**A.** Cisco Catalyst SD-WAN has achieved these industry-focused certifications:

- Cisco SD-WAN for Government (FedRAMP)
- **MEF SD-WAN 3.0 (Service Provider):** <https://www.mef.net/certify/certifications-for-technologies/technology-registry/?orgid=001U0000007OcrIIAS>.
- **FIPS-140-2:** <https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/fips-140.html>.
- **PCI-DSS:** <https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/2984>.
- **CAIQ Attestation:** <https://cloudsecurityalliance.org/star/registry/cisco-systems/services/cisco-sd-wan/>
- **Common Criteria:** <https://www.commoncriteriaportal.org/products/>.

## Services and resources

**Q.** Are any services available to support my SD-WAN solution?

**A.** Regardless of where you are in your journey, Cisco Services offers a full lifecycle of services to support your transition. Our portfolio allows you to create a roadmap for success, speed deployment, and maximize network performance, security, uptime, and efficiency. Cisco experts will help you build your in-house IT expertise and effectively migrate and manage your SD-WAN solution to achieve high service levels at lower costs. [Learn more.](#)

**Q.** Where can I find more information on Cisco Catalyst SD-WAN?

**A.** For more information about Cisco Catalyst SD-WAN, visit <https://www.cisco.com/go/sdwan>.

---

**Q.** What voice and application optimization features does Cisco Catalyst SD-WAN support?

**A.** Cisco has the only SD-WAN solution with fully integrated unified communications support.

- For voice optimization, Cisco Catalyst SD-WAN supports Forward Error Correction (FEC) and packet duplication.
- For internet optimization, Cisco Catalyst SD-WAN supports TCP optimization.
- For on-premises applications, Cisco Catalyst SD-WAN support SLA-based dynamic routing based on real-time network telemetry.
- For SaaS applications, Cisco provides dynamic routing based on cloud and internet telemetry.

**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
Singapore

**Europe Headquarters**  
Cisco Systems International BV Amsterdam,  
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at <https://www.cisco.com/go/offices>.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)