

Cisco+ Secure Connect

Securely Access Applications And Resources
Hosted Anywhere

October 20, 2022

Contents

Product overview	3
Features and benefits	5
Customer Support	6
Document history	7

Securely Access Applications and Resources Hosted Anywhere

Product overview

The new era of hybrid work requires a new approach, and SASE (secure access service edge) is a key enabler of any organization’s hybrid-work strategy. SASE combines networking and security functions in the cloud with campus, branch, remote worker, and contractor (B2B) connectivity to deliver a secure, seamless user experience, anywhere users work – office, home, or coffee shop. But deploying SASE can be complicated. Connecting existing branch SD-WAN appliances and the myriad of user endpoints to a cloud-based fabric requires planning, integration, and configuration.

Cisco+ Secure Connect is a turnkey SASE offer that radically simplifies the way companies can securely access applications and resources hosted anywhere – across multiple public and private clouds – from any location at any time. Easy to deploy, use, and manage through a unified cloud dashboard, it significantly reduces organizations’ operational complexities to deliver greater agility, speed, and scalability.

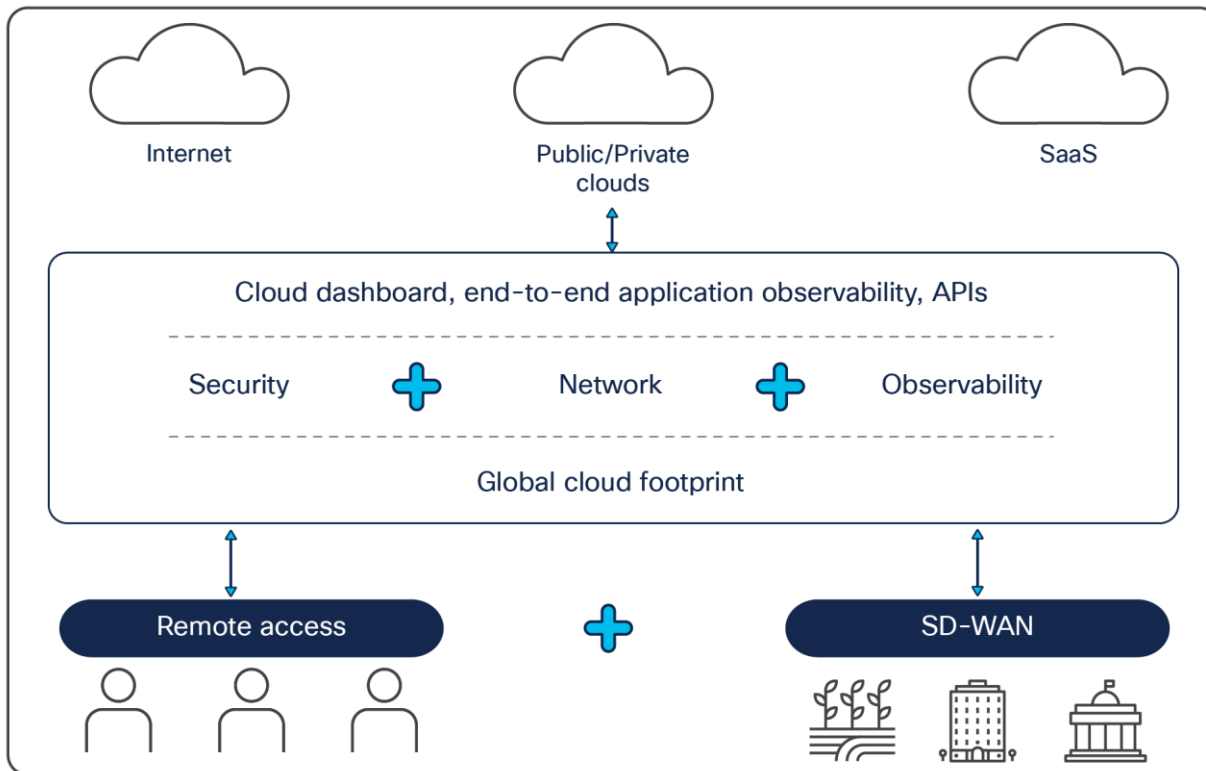


Figure 1.
Cisco+ Secure Connect Use Cases

Cisco+ Secure Connect securely connects users anywhere (in the branch or remote), to any application (in the private data center, public cloud, or SaaS) with a single subscription. The solution integrates client-based and clientless remote worker access, native Cisco Meraki® SD-WAN connectivity, and comprehensive cloud-based security capabilities with ZTNA. Currently, Cisco+ Secure Connect supports up to a maximum of 5,000 concurrent remote users. Some exceptions can be granted, please reach out to your account team for more details. The ceiling on the number of concurrent remote users allowed will increase in the future.

Cisco+ Secure Connect is offered in packages that make it easy for customers to choose the right level of protection and coverage for their organizational needs. There are currently two packages: Cisco+ Secure Connect Essentials and Cisco+ Secure Connect Advantage.

Table 1. Core offer packages

Package	Description	Features
Essentials	Securely connect to users and applications	<ul style="list-style-type: none"> • Remote access / ZTNA: client-based access, clientless browser-based access (up to 10 applications), granular user and application-based access policy, SAML authentication, built-in IdP, posture and contextual access control, reporting • Security: secure web gateway (proxy and inspect web traffic URL filtering, secure malware analytics - up to 500 samples per day), cloud access security broker (cloud application discovery, risk scoring, blocking, cloud malware detection for two applications), L3-L4 cloud firewall, DNS-layer security • Connectivity: private access, network access control, direct SaaS and IaaS peering, Cisco Meraki Secure SD-WAN integration, interconnections of sites, users, and applications • Management dashboard: simplified management and unified visibility of connectivity and security powered by Cisco Meraki • Support: 24x7 support access through email and phone, access to documentation portal for self-help
Advantage	Data protection, advanced policy	<p>All features included in Cisco+ Secure Connect Essentials, plus:</p> <ul style="list-style-type: none"> • Remote access/ZTNA: clientless browser-based access (up to 300 applications) • Security: L7 cloud-delivered firewall + IPS, inline data loss prevention, cloud malware detection (for all supported applications), secure malware analytics (unlimited sandbox submissions).

Features and benefits

Table 2. New features and benefits

Feature	Benefit
Native Meraki SD-WAN integration	Easily connect your branch sites to Cisco+ Secure Connect with the built-in native Meraki SD-WAN integration for access to the internet, SaaS, and private applications. Leveraging the auto VPN capability of your Meraki Secure SD-WAN appliance at your branch sites for connectivity to the SASE fabric provides increased resiliency and intelligent path selection. This also enables the organization to implement consistent access and security controls across all connected sites.
Clientless zero-trust network access (ZTNA)	Cisco+ Secure Connect enables least privileged access control to private applications without requiring any agent or client installed on the endpoint device. Administrators can easily assign access privileges for contractors and employees only to resources they need access to, without any lateral move capability. Administrators can configure posture profiles for endpoint OS type and version, browser type and version, and geolocation information to be used in the access decision.
Client-based secure remote work	Cisco+ Secure Connect enables remote users to access private applications from anywhere through the Cisco+ Secure Connect fabric using a Cisco AnyConnect® client. Identity-based access control is possible using SAML authentication through customer's IdP (identity provider). Endpoint posture is also evaluated; enables granular access control to private resources.
Secure internet access	<p>Secure internet access provides safe access to the internet anywhere users go, even when they are off the VPN. Before the user is connected to any destination, Cisco+ Secure Connect acts as your secure onramp to the internet and provides the first line of defense and inspection, with hybrid protection on the edge and in the cloud. Regardless of where users are located or what they're trying to connect to, traffic can go through the fabric first. Once the traffic gets to the cloud platform, there are different types of inspection and policy enforcement that can happen, based on the security needs of the traffic.</p> <p>With Cisco+ Secure Connect includes a secure web gateway, cloud-delivered firewall, DNS-layer security, a cloud-access security broker, and data-loss prevention. This robust security solution receives real-time proactive threat updates from Cisco® Talos® Intelligence, keeping your users secure while alleviating your IT team from this tedious process.</p>
User authentication	Cisco+ Secure Connect enables customers to either bring their own SAML provider for end-user authentication to the service or use the bundled cloud-identity platform for easy configuration of users and quick onboarding of the service. Cloud-identity capability can be leveraged by customers who don't have a SAML IdP configured or do not want to use their existing SAML IdP for the user authentication to access the service. The cloud-identity capability can be configured through a few easy steps from the Cisco+ Secure Connect dashboard, or an existing Meraki cloud Auth configuration can be simply applied to the service with a single click.
Unified management	The Cisco+ Secure Connect management is handled through a single dashboard to configure, monitor, and troubleshoot the service. Configuration is simplified with guided flows and dynamic checklists. Monitoring of users and sites occurs in a single pane of glass that unifies security and connectivity indicators.

Feature	Benefit
Network interconnect	Network interconnect provides intelligent routing between sources and destinations connected to Cisco+ Secure Connect. Any node connected to the interconnect seamlessly gains access to any already-connected node pending access policy-enforced in a hybrid way across the edge and the cloud fabric. This drastically reduces network complexity, providing a highly available network fabric with minimal setup and maintenance.

Document history

New or Revised Topic	Described In	Date
Changed services to reflect new customer support hours/availability		10/20/22

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)