Cisco+ Secure Connect

Securely Access Applications and Resources Hosted Anywhere

April 2023

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, unified 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.

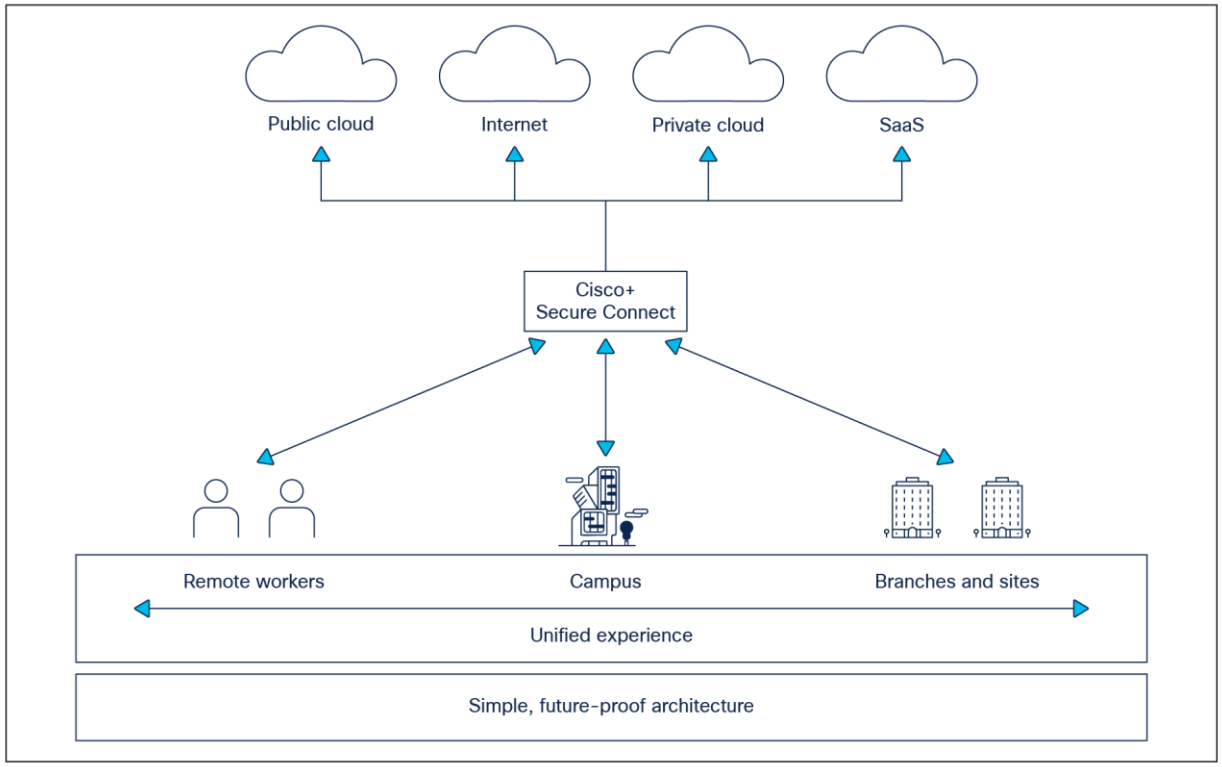

Figure 1.
Cisco+ Secure Connect use cases

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, comprehensive cloud-based security capabilities with Zero-Trust Network Access (ZTNA), enhanced traffic acquisition, and Cisco Meraki SD-WAN policy import, with unified policy on the near horizon for enhanced posture.

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, so they can SASE their way. 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	• 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 Identity Provider (IdP), posture and contextual access control, reporting • Security: Secure web gateway (proxy and inspection of 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), Layer 3 and Layer 4 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 unified SASE support access through email and phone, access to documentation portal for self-help
Advantage	Data protection, advanced policy	All features included in Cisco+ Secure Connect Essentials, plus: • Remote access/ZTNA: Clientless browser-based access (up to 300 applications) • Security: Layer 7 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 AutoVPN capability of your Meraki 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.
Enhanced Meraki SD-WAN cloud traffic acquisition	Cisco+ Secure Connect introduces a dynamically scalable high-bandwidth headend solution for the Meraki SD-WAN integration. Leveraging Meraki's AutoVPN solution, this enhanced cloud traffic acquisition solution dynamically scales bandwidth per connecting Meraki SD-WAN site. The current bandwidth scale per site is approximately 500 Mbps, both unidirectional and bidirectional. This solution also offers an even more simplified user experience for integration of Meraki SD-WAN with Cisco+ Secure Connect.
Clientless Zero-Trust Network Access (ZTNA)	Cisco+ Secure Connect enables least privileged access control of 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 the customer's IdP. Endpoint posture is also evaluated; this enables granular access control to private resources.
Secure internet access	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. Cisco+ Secure Connect includes a secure web gateway, a 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 freeing your IT team from this tedious process.
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.

Feature	Benefit
Meraki policy import	Cisco+ Secure Connect natively introduced a policy import feature that is specifically designed for those who currently have their remote workforce access company resources via remote access connections to the Meraki MX headend. If those customers are transitioning to Secure Connect remote access services, this feature will allow them to import their MX firewall policies affecting client VPN traffic to Secure Connect's cloud firewall via a guided wizard. This will help reduce the amount of time required for administrators to create and streamline their policies. Furthermore, it detects duplicates before the migration.
Unified management	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.
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, with access policy -enforced in a unified way across the edge and cloud from Cisco+ Secure Connect. This drastically reduces network complexity, providing a highly available network fabric with minimal setup and maintenance.

Customer support

Cisco+ Secure Connect now offers 24x7 customer support by calling +1.617.206.4332 or by opening a support case from the product dashboard.

Document history

New or Revised Topic	Described In	Date
Changed services to reflect new customer support hours/availability	Page 6	October 20, 2022
Made tweaks to Product Overview, including use case graphic	Page 3	March 29, 2023
Added additional Features and Benefits	Page 5, 6	March 29, 2023

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**.

Printed in USA C78-3040871-03 04/23