Cisco Secure Access China Operated by Digital China Cloud

Safeguarding Your Hybrid Workforce

March 2025

Contents

Mainland China represents a critical market for most multinational companies. For these customers, establishing a presence in the country drives significant business and operational opportunities that stems from embracing collaboration and hybrid work environments within their domestic operations and with the rest of their global organization. Succeeding in this complex landscape demands solutions and innovations that ensure online security and compliance with local regulations.

Security Service Edge for China

Security Service Edge (SSE) is a key enabler of any organization's hybrid-work strategy. As a multi-layered defense, SSE combines multiple security functions in the cloud to protect users working anywhere in China as they access resources everywhere—in public SaaS applications (apps), private apps in data centers and private clouds, and across the internet. End users are assured of a secure, transparent experience, anywhere they work — at the office, at home, or on the road.

To improve the customer's security posture, an SSE solution in China must deliver policy enforcement with superior user experience, reduced IT complexity, and improved security efficacy. All the while, the organization must navigate through regulatory requirements. A regulatory compliant solution that allows organizations to pursue their growth objectives while safeguarding their employees is, therefore, essential.

Cisco Secure Access China Operated by Digital China Cloud

Operated by Digital China Cloud (DCC), Cisco Secure Access China is a cloud-delivered security SSE solution providing seamless, transparent, and secure access from anything to anywhere within mainland China. It is built with compliance in mind to help organizations bridge their global operations with the Chinese dynamic market. Secure Access China offers the same advantages as Cisco Secure Access global in providing critical core SSE components with extended capabilities including VPN-as-a-Service (VPNaaS), integrated inline DLP, Intrusion Prevention System (IPS), and threat detection powered by Talos – in a simple license and management platform. Organizations can now protect their users inside China as they seamlessly access all their needed resources and apps. See figure 1.

Cisco Secure Access China features common administrative controls, data structures, and policy management that eases interoperability with other products from Cisco and third-party vendors. For instance, Secure Access China allows use of a variety of SAML Identity Providers (IdPs) and Active Directory. It integrates with other Cisco offerings including SD-WAN as permitted by China's regulated environment.

Secure Access China increases security to reduce risk, ensures compliance while simplifying IT operations in China, and provides users with frictionless access to raise productivity.

Figure 1.
Cisco Secure Access China capabilities

Better for Users

Secure Access China streamlines the user experience when in China, roaming around, or traveling into the country. Users can quickly authenticate and access their desired applications which boosts productivity and eliminates tendencies to circumvent security procedures thereby minimizing risks and disruptions. With the familiar Cisco Secure Client, users in China can connect, authenticate and go straight to their desired applications.

With Secure Web Gateway (SWG) in China, employees get consistent and secure internet access whether they are in the office or on the go. All web traffic can be monitored and protected against threats, maintaining security without compromising performance. When deployed and configured on both Secure Access global and China regions, international roaming users traveling into China automatically can use Secure Access China and apply user and group policies that can comply with China regulations. Correspondingly, China users roaming abroad can connect to their global instance.

Easier for IT

Cisco Secure Access global deployment simplifies and automates security operations and adoption. IT teams benefit from this capability to centralize policy management. To ensure strict compliance with Chinese data sovereignty and localization, Secure Access China is intended to prioritize and meet this requirement to mitigate costly regulatory risks, penalties, and possible reputational impact. Secure Access China administration uses the familiar dashboard to simplify training and use of the management tool. Data reports, alerts, and logs are stored inside China by default. Alternatively, administrators can opt to save or establish their own customer-managed storage.

Safer for Everyone

Cisco Secure Access China follows the global defense-in-depth architectural approach to counter sophisticated cyber threats. This robust approach ensures end users are safeguarded against infected files, malicious websites, nefarious attacks, and common threats like phishing and ransomware. This translates into a significant reduction of the attack surface and allow IT and security teams to enforce least privilege controls effectively and strengthen their security posture across the organization.

With Security Access China, IT teams can have enhanced visibility into its network activities in the country, identifying and blocking unsanctioned application usage, protecting from data leaks, which can otherwise compromise organizational security. An added advantage and extra layer of security is the use of network

segmentation in China along with a combination of available features such as strict access controls and intrusion prevention to effectively secure internal resources and prevent bad actors from even discovering their presence. This proactive defense mechanism not only protects sensitive data but also maintains business continuity and fosters a secure and efficient environment for managing operations within China's unique regulatory landscape.

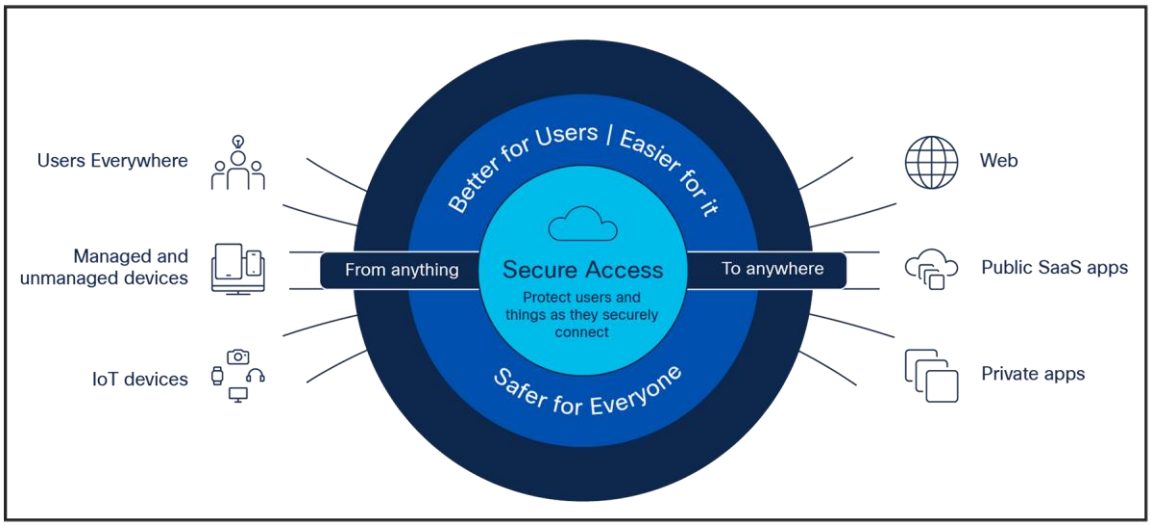

Figure 2.
Secure connectivity from anything to anywhere

Features and Benefits

Table 1. Features and Benefits

Feature	Benefits
VPN-as-a-Service (VPNaaS)	Having broader compatibility, Virtual Private Networks (VPN) is a proven choice for deployment across diverse environments without significant changes to existing infrastructure and operations. Secure Access China provides cloud-delivered VPN to give users comprehensive secure access to resources, private servers, including secure access for non-web internet traffic. • IT simplification (Local IP Pool, multiple VPN profiles). • Identity-based access control using multiple authentication methods including SAML, RADIUS, and certificate. • Endpoint posture evaluation increases the granularity of access control. • Simplifies connectivity with no need to select head-end or tunnel type. • Functionality examples: split tunneling and tunnel all support, peer-to-peer communication, trusted network detection.
Secure Web Gateway (SWG)	Log and inspect all web traffic (http/https) for greater transparency, control, and protection. IPsec tunnels, PAC files and proxy chaining are used to forward traffic for full visibility, URL and application-level controls, and advanced threat protection. • Content filtering by category or specific URLs to block destinations that violate policies or compliance regulations. • Scan downloaded files for malware and other threats. • File type blocking (e.g., block download of .exe files).

Feature	Benefits
	• Full or selective TLS decryption to protect from hidden attacks and infections. • Granular app controls to block specific user activities in select apps (e.g., file uploads to Dropbox, attachments to Gmail, post/shares on Facebook). • Detailed reporting with full URL addresses, network identity, allow or block actions, plus the external IP address. • Protection of internet-based SaaS apps with customizable controls and traffic path options.
Cloud Access Security Broker (CASB)	• Detect, report on, and block selected cloud apps in use. Manage cloud adoption and block use of offensive, non-productive, risky, or inappropriate cloud apps to reduce risk. • Discover, block, and revoke authorization of risky plug-ins and extensions from OAuth-based authorization to Microsoft 365 and Google tenants. • Reports on vendor category, application name, and volume of activity for each discovered app. • App details and risk information such as web reputation score, financial viability, and relevant compliance certifications. • Tenant restrictions to control the instance(s) of SaaS apps that groups/individuals can access.
Data Loss Prevention (DLP)	Inline or Real Time Data Loss Prevention (DLP). Analyze data in-line to provide visibility and control over sensitive data leaving the organization. Unified policies and reporting for more efficient administration and regulatory compliance. • 1,200+ built-in global identifiers for Personally Identifiable Information (PII), spanning 77 countries, for compliance with Personal Health Information (PHI), GDPR, HIPAA, PCI, and more. • Integrates with on-premises DLP solutions for centralized event management and remediation workflows. • User-defined dictionaries with custom phrases (such as project names). Detection and reporting on sensitive data usage and drill-down reports to help identify misuse.
Advanced Malware Protection	Prevents, detects and blocks files with known bad reputation. Enriches security protection by detecting and remediating malicious files before they reach an endpoint. • Increases effectiveness and efficiency of security administrators. Blocks known malware exploits and other threats in the form of viruses, worms, Trojans, adware, etc.
Firewall as a Service (FWaaS) **with** **Intrusion Prevention System (IPS)**	Provides full visibility and comprehensive security controls for traffic between users and the destinations/apps, on the Internet or in customer's private infrastructure, across all ports and protocols. Includes remote users access the Internet or to private apps while they are roaming or from a branch office campus network. • L3/4 access control rules for securing users/groups, networks or devices to access Internet, private networks and/or private apps. • Customizable IPS profiles with Snort 3.0 support. Enforce per rule IPS inspections on traffic patterns matched by a rule, for both Internet and private access. • Visibility and control over Layer 7 apps, application protocols and ports/protocol, with a constantly growing base of apps identified. • Decrypts prior to inspections, for Internet or private access traffic. • Bi-directional file inspection and file type controls for traffic between users and private apps. Scalable cloud compute resources eliminate appliance capacity concerns.
Talos threat intelligence	Uses Cisco Talos, one of the world's largest commercial threat intelligence teams with a massive database of threat data and analysis to identify cyber threats and improve incident response rates.

Feature	Benefits
Management and reporting console	Secure Access China unified security policy creation and management, using intent-based rules, across internet, public SaaS app, and private app access. Provides extensive logging and the ability to export logs to enterprise Security Operations Center (SOC). • Single place to define policy for any user to any app. Simplifies the process of building security policies and drives consistency in policy definition for entire China organization. • Unified source (users, devices) and unified resources (apps, destinations) allow the security policy to follow the users no matter the point of attach and or which app they access. • Reduces on-going policy management activities. • Improves visibility and time-to-detection with aggregated reporting. Simplifies the overall SOC/security analyst investigation process.
Device support	• Cisco Secure Client included with Secure Access China at no added costs. • Secure Client on Windows and MacOS for internet traffic, private traffic via VPNaaS. • Cisco Security for roaming users with SWG protection.
Integration with Catalyst SD-WAN: branch users access the Internet/SaaS apps	Integration and automation between Catalyst SD-WAN and Secure Access enables steering from branch users to the web and SaaS apps to be protected by Cisco Secure Access. • Increased threat protection from Secure Access's multi-layer security solution. • Tunnel automation between branch SD-WAN locations and Secure Access, simplifying deployment for IT. • More consistent experience when users move between roaming and on-premises locations. • Simplifies IT/security operations with Secure Access's centralized policy administration, easy up/down scalability, and relief from capacity constraints

Packaging options

Cisco Secure Access China has two primary tiers: Secure Access Essentials and Secure Access Advantage. Both tiers are available for two use cases—Secure Internet Access (SIA) and Secure Private Access (SPA)—purchased as part of a single subscription and delivered as a single, unified dashboard and service. A customer may choose to purchase one or both use cases in a tier. The table below provides a high-level comparison:

Table 2. License packaging

Category	Features	Essentials	Advantage
Secure Access	Secure Internet Access (SIA) ▪ Roaming module (Web) ▪ SD-WAN DIA ▪ Secure Client VPN ▪ PAC, Proxy Chain	✓	✓
	Secure Private Access (SPA) ▪ Secure Remote Access (RAVPN) ▪ In-country Branch-to-Branch, RAVPN-to-Branch	✓	✓
Foundational Security	Firewall-as-a-Service for Layer 3 & Layer 4 controls of web and private apps	✓	✓
	Secure web gateway (proxy web traffic, URL filtering, content filtering, advanced app control)	✓	✓

Category	Features	Essentials	Advantage
	CASB cloud app discovery, risk scoring, tenant controls	✓	✓
Advanced Security	Layer 7 cloud firewall		✓
	Intrusion Prevention System (IPS) protections		✓
	Data Loss Prevention (DLP) for web applications, real-time (In-line only)		✓
Support	Includes 24x7 solution support access via email and phone provided by tiered Partner & Cisco support	24 x 7	24 x 7

Cisco Secure Access China Solution Support Service

The first line of support for Cisco Secure Access China is provided locally by DCC as the operator of the service. In partnership with Cisco TAC support team, Secure Access China includes a separate SKU for Solution Support.

- Technical Support (24x7 access) via DCC ticket portal and/or phone support
- 30-minute response time for Severity 1 and Severity 2 cases
- Chinese language support
- Technical on-boarding and adoption assistance

Additional information

For more information, please visit: [Cisco Secure Access China]

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 Cxx-xxxxxx-00 03/25