Cisco Secure Access

Protect Your Hybrid Workforce with Cloud-Agile Security

August 2025

Contents

Hybrid work and Security Service Edge

Today's hybrid work environments require a revised approach to security, and SSE (Security Service Edge) is a key enabler of any organization's hybrid-work strategy. SSE combines multiple security functions in the cloud to protect users working anywhere 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 user experience, anywhere they work — office, home, or on the road. For the highest effectiveness, SSE solutions must deliver a superior user experience, reduce IT complexity, and improve security efficacy.

Cisco Secure Access product overview

Cisco Secure Access is a cloud-delivered SSE solution, grounded in zero trust, that provides seamless, transparent, and secure access from anything to anywhere. It provides all core SSE components (ZTNA, SWG, CASB, and FWaaS) plus extended capabilities including VPN-as-a-Service (VPNaaS), DLP, AI Assistant, visibility/control/guardrails for generative AI use, DEM, reserved IP, RBI, DNS Security, and much more—in one license and management platform.

Organizations can protect users as they seamlessly access their needed resources and apps, regardless of protocol, port, or level of customization. See figure 1.

Cisco Secure Access 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 integrates with a wide variety of SAML Identity Providers (IDPs) such as AD, Azure AD, Okta, Ping, etc. It integrates with other Cisco offerings including SD-WAN, Splunk, XDR, Thousand Eyes, third party technologies such as Menlo Remote Browser Isolation, Chrome Enterprise Browser, and AppOmni for SSPM.

Secure Access increases security to reduce risk, simplifies IT operations to lower complexity, and provides frictionless user access to raise productivity.

Cisco Secure Access DNS-Defense offers an ideal solution for organizations interested in DNS-layer security, either alone or as an initial step toward SSE (see package options at the end). It rapidly evaluates DNS requests, blocking access to malicious domains and threats before they reach your network and endpoints. This rapidly improves your security posture while reducing alert pressure for your security team.

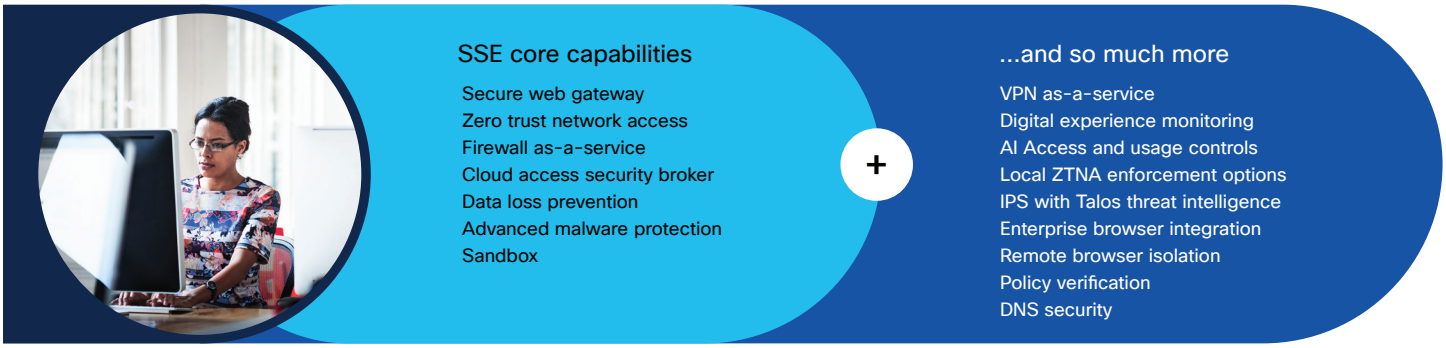

Figure 1. Cisco Secure Access capabilities

Better for users

By dramatically improving the user experience, Secure Access not only increases user productivity but also reduces user temptation to circumvent security procedures that increases risk. A single, unified client simplifies how users connect; they authenticate and go straight to the desired app.

For private app access, users automatically and transparently connect via ZTNA or VPNaaS, without extra steps or cumbersome verification tasks. This minimizes the user hassles as there's no need to launch multiple clients with different sign-on processes.

Easier for IT

IT teams struggle with a plethora of security tools, multiple management consoles and policy engines, and several software agents for various user and device types. These challenges are magnified by the separate reporting, alerts, and incidents that arise from each security point product.

Cisco Secure Access simplifies and automates operations via a single, cloud-managed console, unified client, centralized policy creation process, and aggregated reporting. Instead of disparate products, IT only manages one tool for granular control of users across locations, as they access apps anywhere, from managed and unmanaged devices. IT does less manual aggregation as they rapidly detect and block threats, expedite investigations, and minimize remediation tasks, while deepening visibility into end user activity.

Safer for everyone

Cisco Secure Access's defense-in-depth architectural approach, which secures against sophisticated cyber threats, has garnered recognition for industry-leading security efficacy. End-users are protected from infected files, nefarious websites, phishing and ransomware schemes. IT and security teams can reduce the attack surface, enforce least privilege controls, enable posture validation, and eliminate security gaps in distributed environments. They gain visibility into and block unsanctioned app usage. Cloaking internal resources and preventing hackers from discovering their presence generates an extra layer of security.

Cisco Talos threat intelligence fuels this functionality with its unrivaled telemetry, extensive research, and advanced AI to identify and help stop threats and speed remediations. By mitigating risk, organizations maintain business continuity and avoid the reputation and financial impact of a breach.

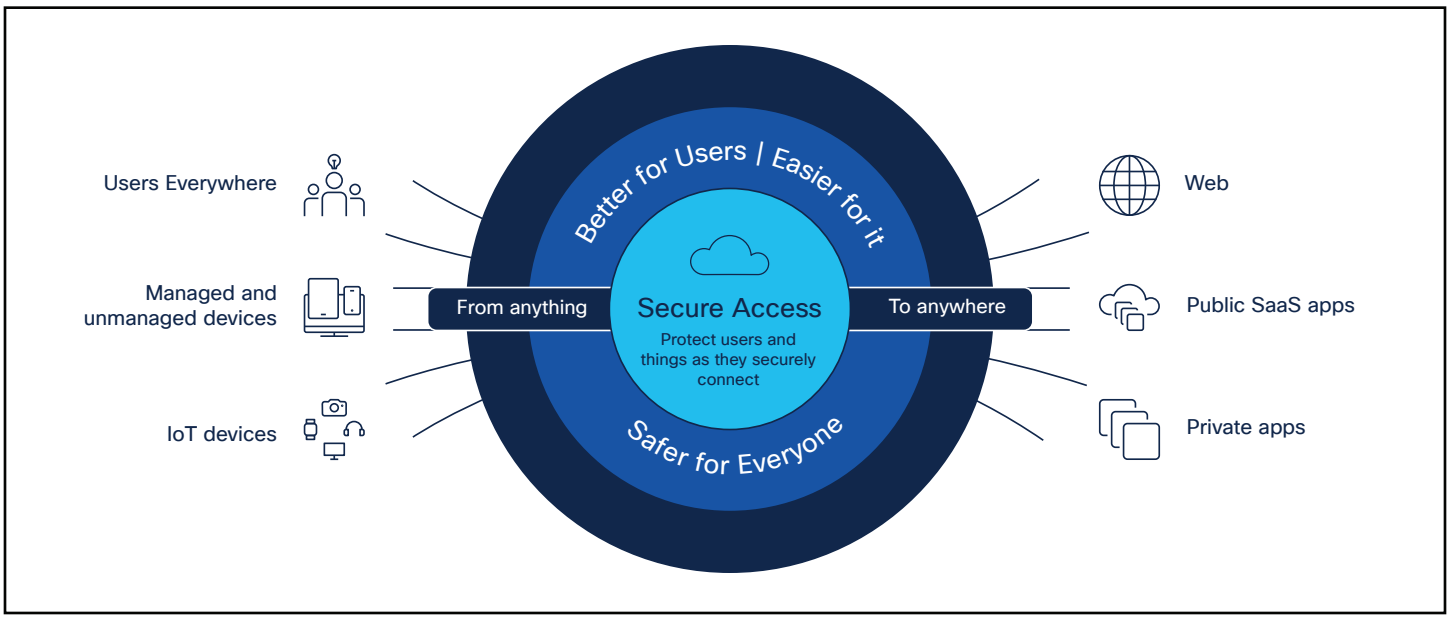

Figure 2. Secure connectivity from anything to anywhere

Features and benefits

Feature	Benefit
Zero Trust Network Access (ZTNA)	Provide granular, app-specific secure access to private apps in on-premises data centers or in cloud environments, with the flexibility to choose cloud or local enforcement. Its identity aware proxy design uses least privilege principles and contextual insights to granularly deny access by default and grant access to apps when policy explicitly grants it. ▪ Client-based access via the Cisco Secure Client, the single, unified client for Secure Access. ▪ Clientless access (via browser) protects traffic to web apps (http/https) and private apps with browser-based SSH and RDP protocol support, which significantly expands the apps that can be protected via clientless ZTNA. ▪ Establishes per-session secure access after a device posture check. ▪ Authenticates users through a secure, encrypted tunnel, so users see only apps they have permission to access (prevents lateral attacker movement).

Feature	Benefit
	• Application proxy provides transparent, secure remote access without exposing apps to the Internet and hides network details from clients using the apps. Prevents nefarious IP reconnaissance even if a device was compromised. • Implements device-specific access control policies, preventing possibly compromised devices from connecting to its services. • Administrators have extensive policy "levers" to specifically assign the right access to the right users. Examples include assigning distinct privileges for contractors vs. employees or creating posture profiles that evaluate diverse endpoints and browsers. • Enhance visibility and streamline the discovery of private resources. By monitoring private network traffic and analyzing usage patterns, it provides actionable insights and an intuitive workflow for administrators to discover and define private resources.
VPN-as-a-Service (VPNaaS)	Not all private apps can be secured by ZTNA. With its VPNaaS option, Secure Access provides cloud-delivered secure access to all private apps (not just some), including those apps not supportable by ZTNA. Additionally, VPNaaS can secure access for non-web internet traffic. • User ease of use (always on VPN, start before logon). • 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. • Integration with Identity Services Engine (ISE), to leverage SGT's and RADIUS Change Of Authorization (COA). • Functionality examples: split tunneling and tunnel all support, peer-to-peer communication, trusted network detection, BYO certificate, split DNS, dynamic split DNS.

Feature	Benefit
Secure Web Gateway (full proxy)	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. • Sandboxing analyzes unknown files (see dedicated section for Cisco Secure Malware Analytics). • File type blocking (e.g., block download of .exe files). • 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. • Multimode 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, including generative AI. Manage cloud adoption and block use of offensive, non-productive, risky, or inappropriate cloud apps to reduce risk. Multimode capabilities to detect, log and control user/group activities. • 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. • Discover and control usage or attempted usage of 720+ generative AI apps. Block usage or create and enforce policies to control how these apps are used.

Feature	Benefit
Data Loss Prevention (DLP)	Multimode Data Loss Prevention (DLP). Analyze data in-line to provide visibility and control over sensitive data leaving your organization. API-based functionality for out-of-band analysis of data at rest in the cloud. 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. • Identifiers for cloud service providers (AWS, GCP, Azure) session and API tokens, keys, and secrets. • 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. • API-based content inspection functionality supports Microsoft 365 (SharePoint and OneDrive), Google Drive, Webex, Box, Dropbox, Slack, ServiceNow. • Extend real-time (inline) DLP policy to private resource traffic, allowing you to secure data stored in private applications, preventing unauthorized downloads and ensuring files containing sensitive data aren't stored in inappropriate locations.
AI Access	Enables employees to safely use generative AI applications and model repositories, thus generating the AI productivity lift while mitigating risk. • Enables visibility and control of 1200+ LLMs to control Shadow AI usage. • Establishes guardrails to mitigate toxic content and prompt injection attacks from popular LLMs. • Controls or blocks ingress and egress of source code via Web and API interfaces for generative AI such as ChatGPT. • Machine Learning-based DLP identifies and protects documents like patent applications, non-disclosure agreements, merger and acquisition related content. • Uses pre-enforcement controls to identify and block potentially risky models from AI repositories.

Feature	Benefit
Hybrid Private Access	Multiple options (cloud or on-premise) for ZTNA traffic routing and policy enforcement provide optimal performance and granular security, with one, simple user experience. Local enforcement can be easily enabled on existing Cisco firewalls. • Optimized user experience – Branch and campus firewalls provide a direct path to applications for in-office employees without hair-pinning to the cloud, saving on cloud costs and providing high speed access to apps. • Integrated privacy and compliance – Employee connection to designated (sensitive) apps can be inspected locally with an on-premise firewall instead of the cloud. • Business continuity/disaster recovery – Ability to select between two private traffic routes and enforcement points provides flexibility and business/security resilience.
Cisco identity intelligence (CII)	Identity trust levels are incorporated directly into the Secure Access dashboard. Today, this provides administrators with immediate access to valuable identity-related insights. This capability is foundational for future enhancements that will enable policy enforcement based on CII user trust levels for private and internet applications.
Cloud malware detection	Detects and removes malware from cloud-based file storage apps. Enriches security protection by detecting and remediating malicious files before they reach an endpoint. • Increases effectiveness and efficiency of security administrators. • Once activated, all files in cloud-based services will be hashed and sent for malware scanning automatically. Any file containing malware will be flagged so a security admin can remediate, including quarantine and/or deletion. • Supports Box, Dropbox, Webex, Microsoft 365, and Google Drive, AWS S3, Azure.

Feature	Benefit
AI Assistant	Generative AI capability that helps security administrators save time, improve operational efficiency, and reduce complexity. Policy assistant automatically converts conversational, English phrases into specific security policies. • Multi-person administrator groups can create a more consistent and effective policy set. • Magnifies cost reductions and resource savings when large sets of policies are needed. Document assistant simplifies finding and understanding documentation, making it easier to quickly get answers to Secure Access questions. • Interprets questions phrased in natural language and provides answers from Secure Access documentation. • Handles complex queries that involve looking up multiple documents and pages to deliver comprehensive responses. Troubleshooting assistant automates troubleshooting workflows for private resource access issues via VPN or ZTNA, correlates results from various subsystems, and provides a concise analysis summary. Designed to significantly reduce the time and effort required to diagnose and resolve issues.
Experience Insights: Digital Experience Monitoring (DEM)	Monitor health and performance of endpoints, apps, and network connectivity as users access resources. Optimize user productivity, simplify troubleshooting, and reduce time to resolution of incidents by automatically capturing details on the user's end-to-end experience. Integrated AI-driven insights help you proactively identify and mitigate potential performance issues, ensuring a more resilient environment. Key insight examples: • Endpoint performance – CPU utilization, memory usage, and WIFI signal strength. • Network performance – Segment visualization from the endpoint to Secure Access, including metrics such as latency, jitter, packet loss, and suggested remediations. • Performance status of commonly used SaaS apps (top 20) including Outlook, Slack, Workday, and SharePoint. • User specific security events. • Performance for collaboration apps including Webex, Zoom, and Microsoft Teams, including historical data and digital experience scores. • Endpoint topology map for the entire organization globally. • Purchasing a ThousandEyes endpoint license enables end-to-end synthetic testing—from any endpoint to both public and private apps—all managed within the Secure Access unified dashboard.

Feature	Benefit
Security policy verification	Configuration changes are one of the leading causes of service-impacting incidents. With policy verification, you can proactively and reactively assess the impact of changes, helping to reduce configuration errors, minimize service outages, and maintain seamless user access. • Proactive Change Management – Analyze the potential impact of planned changes to posture before they are implemented, ensuring smoother roll-outs and fewer disruptions. • Reactive Incident Resolution – Quickly identify and address the root cause of incidents related to configuration changes, reducing downtime and troubleshooting effort. • Fosters operational efficiency and a safer, more reliable Secure Access environment.
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.
Cisco Secure Malware Analytics	Combines advanced sandboxing with threat intelligence into one unified solution to protect organizations from malware. Provides access to the full Secure Malware Analytics console, enabling execution of malicious files in a glovebox, tracking file execution actions, and capturing network activity generated by the file. When combined with Investigate API, security analysts may go further and uncover malicious domains, IPs, ASNs mapped to a file's actions to get the most complete view of an attackers' infrastructure, tactics, and techniques. • Ability to detect hidden attack methods and report on malicious files. • APIs to integrate with XDR and commonly used SIEMs for enriching security data. • Retrospective notification if file disposition changes (originally good/later deemed malicious).

Feature	Benefit
Remote Browser Isolation (RBI)	RBI protects against browser-based threats by shifting the execution of browsing activity from the user to a remote, cloud-based virtualized browser. Website code is run separately, and only a safe version of the web is delivered to the user. Fully transparent to the end user. No need to worry about malware that has not yet had a signature created. • Isolation of web traffic between user device and browser-based threats. • Protection from zero-day threats. • Granular controls for different risk profiles. • Rapid deployment without changing existing browser configuration. • On-demand scale to easily protect additional users. • Protect employees who may need to access known risky internet sites. Productivity is not reduced due to blocking and users stay safe.
DNS-layer security	Filter at the DNS layer to block requests to malicious and unwanted destinations, over any port or protocol, before a connection is established to the network or endpoints. • Protects internet access across all network devices, office locations, and roaming users and mobile devices. • Provides detailed reporting for DNS activity by type of security threat or web content and the action taken. • Artificial intelligence algorithms used by our DNS Tunneling provide real time detection and protection against data exfiltration. • Enables rapid rollout to thousands of locations and users for immediate protection. • Provides visibility in reports and applied policies – down to the user level – by leveraging the Cisco Secure Client, Virtual Appliances, and third-party integrations.
Talos threat intelligence **And** **Investigate API**	Cisco Talos, one of the world's largest commercial threat intelligence teams, continuously runs AI, statistical, and machine learning models against its massive database of threat data and analysis to provide insight into cyber threats and improve incident response rates. Investigate, available via API, leverages Talos data to help security teams programmatically access and analyze this threat intelligence to speed incident investigation and response. Examples include: • Gain insight into the context around threats (domain and IP analysis, threat scores, domain categorizations, historical data). • Map out attacker infrastructure by associating attacks with specific domains, IPs, ASNs, and malware. • Identify emergent threats, predict where future attacks might be staged. • Create custom queries and gain greater context for faster decision making and remediation.

Feature	Benefit
Single management and reporting console	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 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 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.
Resource Connectors	Resource Connectors simplify the administrative tasks to setup secure connectivity to private apps, regardless of whether they are in an on-premises data center or the cloud. Supports AWS, Azure, and VMWare. Additionally, Resource Connectors in Docker Containers provide a cloud-agnostic solution for deploying Resource Connectors, enabling broad connectivity across various environments. • Reduce dependency on network teams for device and firewall rule changes. • Avoid routing complexities, such as setting up dynamic routing or overlapping subnets. • In scenarios such as a merger, networks are often kept separate with overlapping IPs, etc. Using tunnels gets complex. App Connectors can shield this complexity. • Protects private apps by hiding their location (IP address) and only allowing connections through the zero trust policies within Security Access. • Prevents lateral movement by isolating resources and networks.
Device support Cisco Secure Client is included with Secure Access, at no added cost.	• Secure Client on Windows and MacOS for internet traffic, private traffic via ZTNA, private traffic via VPNaaS. • Secure Client on Linux, iOS, Android for internet traffic and private traffic via VPNaaS. • Clientless ZTNA option for private traffic; browser-based (no client). • Cisco Security for Chromebook Client enforces DNS and SWG protection. DNS-layer security for the entire Chromebook OS. • All internet traffic can be sent through the same ZTNA Secure Client module as private traffic, enabling you to take advantage of deep posture assessment and granular policy enforcement.

Feature	Benefit
Chrome enterprise browser integration	Enables an optimized combination of cloud and browser-based security. Organizations can provide a higher level of security and a better user experience to their extended workforce – including part-time employees, partners, and contractors using managed and unmanaged devices. • Unmanaged device access with managed profile based on identity. • Local browser – copy/paste, DLP, watermarking, printing, and screenshot controls. • VDI replacement using enterprise browser and Cisco Secure Access. • 3rd party/consultant/contractor/partner access to private apps.
Mobile device ZTNA support	Cisco collaborated with both Apple and Samsung to create unique, streamlined ZTNA processes with performance and security benefits. Cisco also supports ZTNA from other Android mobile devices. • Secure Access provides efficient enrollment, configuration, troubleshooting, and traffic steering. • Utilizes QUIC and MASQUE protocols for faster transit and VPP acceleration for better throughput. • Simplified deployment with no need to roll out and manage a full client on iOS devices. • Leverages built-in functionality within the iOS operating system and takes advantage of Apple's iCloud private relay with a single layer of encryption for fast, secure access.
Integration with Cisco SD-WAN	Integration and automation between Secure Access and Cisco SD-WAN – Catalyst, Meraki, and Firepower Threat Defense (FTD) – enables customers to choose optimal branch connectivity while enjoying a unified SSE policy and consistent enforcement. • 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. • Use of VPN/VRF and ISE security tags (SGT) from SD-WAN enables Secure Access to enforce different policies based on data in different tags/labels, achieving more granular security protection. Increases consistency of security policy enforcement across the branch and in the cloud.

Feature	Benefit
Integration with Identity Services Engine (ISE)	ISE and Secure Access integration provides granular, identity-based information to deepen visibility into what users are doing, when, and how. It enriches policy control and enforcement for internet and SaaS app traffic to reduce the attack surface of the network and limit potential lateral movement of threats. • Enable more precise enforcement of the right policy, for the right user or device, at the right time. • Support RADIUS for authentication requests with ISE. • Finely segments users and things with Security Group Tags (SGT), often referred to as micro segmentation. • The seamless integration experience between Secure Access and ISE is enabled via Context Service on Security Cloud Control, a core platform providing a standard and consistent representation of SGTs.

Packaging options

Cisco Secure Access is available as a full SSE solution, delivered in a single subscription, with a single policy set, and unified dashboard. Alternatively, Secure Access offers various packages to suit specific needs: DNS Defense for DNS-layer security, Secure Internet Access (SIA) to protect access to the internet and SaaS applications (includes all DNS Defense capability), and Secure Private Access (SPA) to secure access to private applications. Each package comes in “Essentials” or “Advantage” configurations. See the package comparison guide to compare features across packages.

Cisco Secure Access: Software Support Service

Cisco Secure Access requires a separate SKU for Software Support-Enhanced, with the option to upgrade to Software Support Premium.

Cisco Software Support Enhanced

- Technical Support (24x7 access to Cisco Cloud Security Support – phone/on-line).
- Software updates.
- Primary point of contact with software expertise.
- Technical on-boarding and adoption assistance.

Cisco Software Support Premium (optional upgrade)

Includes Enhanced level features plus:

- Prioritized case handling over Enhanced support.
- Assigned expert who provides incident management and proactive consultation and recommendations to ensure successful security software deployment and ongoing management and optimization.
- Support case analytics.

To learn more about Cisco Support Services for Security Software, click here.

For more information

For more information, please visit: Cisco Secure Access.