CISCO
SECURE

Data sheet
Cisco public

Cisco Secure Access

Protect your hybrid workforce with cloud-agile security

May 2023

The bridge to possible

Contents

Protect your hybrid workforce with cloud-agile security

Hybrid work and Security Service Edge

The new era of hybrid work requires 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 both protect employees, contractors or partners who work from any location as well as safeguard critical resources. Whether sessions involve applications in private data centers, SaaS locations, peer-to-peer, IaaS or Internet sites, SSE acts as a 'security intermediary' to identify and prevent multiple types of malicious activity. End users are assured of a secure, transparent user experience, anywhere they work – office, home, or on the road. SSE solutions must address three principal requirements: Deliver a superior user experience, reduce IT complexity, and improve security efficacy.

Product overview

Cisco Secure Access is a converged cloud security SSE solution, grounded in zero trust, that provides seamless, transparent, and secure access from anything to anywhere. This solution ushers in a holistic set of core modules including ZTNA, SWG, CASB and FWaaS. The platform then goes beyond these features and adds multimode DLP, DNS security, remote browser isolation (RBI), sandboxing and Talos threat intelligence. By leveraging these capabilities, all under one cloud-delivered platform, organizations can solve a variety of security challenges. Users can now safely and seamlessly access all the resources and apps they need, regardless of protocol, port, or level of customization.

Cisco Secure Access is designed with common administrative controls, data structures, and policy management that eases interoperability with other synergistic components. For instance, this solution works fine with other Cisco offerings including SD-WAN, XDR and digital experience monitoring as well as third party technologies to improve customer outcomes.

Secure Access enforces modern cybersecurity, while fundamentally reducing risk, radically simplifying IT operational complexity, and minimizing tasks performed by end-users.

Better for users

Cisco Secure Access dramatically improves the user experience to remove friction, overcomes potential side-stepping of necessary security procedures, and increases productivity. The solution utilizes a unified client that simplifies the way users connect; they authenticate and go straight to the desired application. Such an "all-access" feature automatically connects them with least privileged concepts, preconfigured security policies and adaptable enforcement measures that administrator's control.

Whether sessions utilize ZTNA or VPNaaS for specific non-standard apps, users don't need to take extra steps. Repeating cumbersome verification tasks over and over is prevented. User confusion over such concerns as what access method is required for different resources, if a separate client needs to be launched, or a different sign-on process stipulation, is eliminated. Centralized access to all applications greatly eases the process users take to connect, ensures security, including user and device posture validation, and improves productivity.

Easier for IT

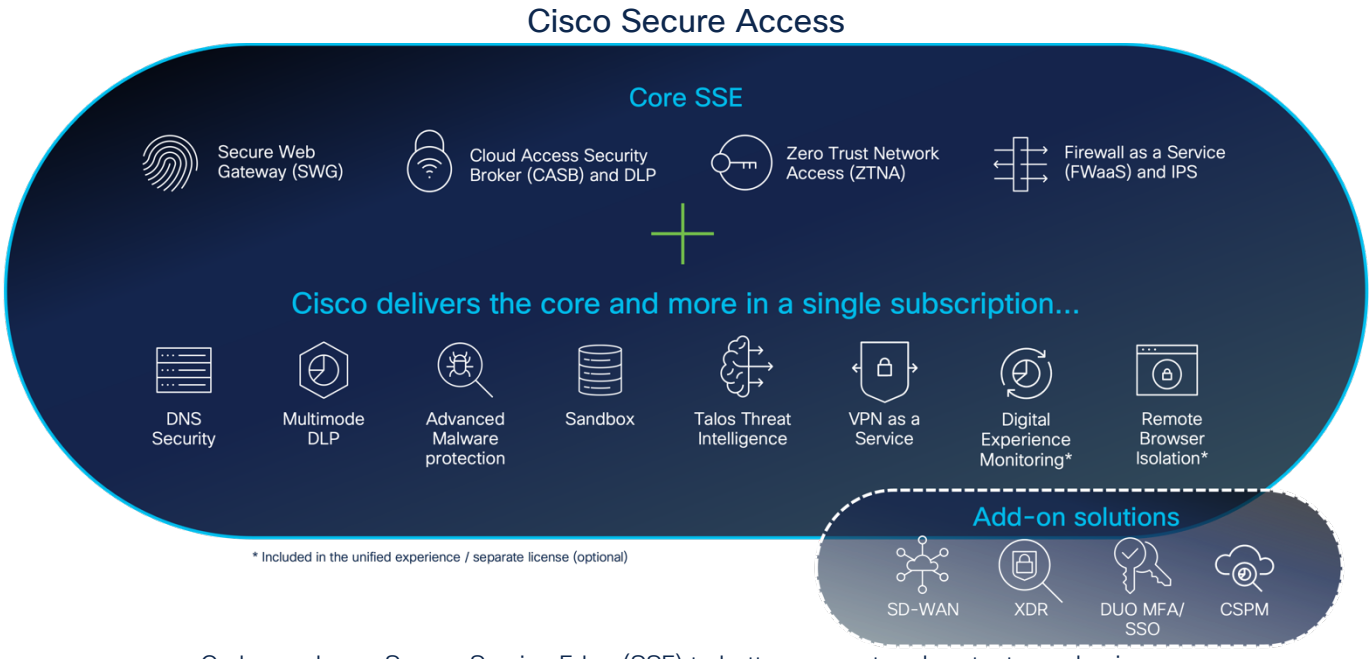
IT teams today struggle with integrating a plethora of security tools, require multiple management consoles and policy engines, and need to deploy and manage several software agents for each end-user device. These challenges are magnified by the separate reporting, alerts and incidents that arise from each security point product.

Cisco Secure Access simplifies and automates operations for security and IT teams via a single, cloud-managed console, unified client, centralized policy creation process, and aggregated reporting. Now instead of deploying numerous disparate products, IT only needs to manage one tool. This translates into measurable efficiency gains, resulting in cost reductions and a flexible IT environment that supports greater business agility. IT can now more rapidly detect and block threats, expedite investigations, and minimize remediation tasks, all while improving visibility into end user activity with less manual aggregation tasks.

Safer for everyone

Cisco Secure Access provides industry leading security efficacy for both end users and on-premises resources. The extended capabilities of its defense-in-depth architectural approach secures against a diverse set of cybersecurity threats. End-users are protected from risks such as infected files, nefarious websites as well as 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.

Security teams can obtain visibility into unauthorized shadow IT operations and unsanctioned applications usage and block such activities. By cloaking internal resources and preventing hackers from discovering their presence, IT achieves an extra layer of security. All this functionality is backed by Cisco Talos threat intelligence 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.



Go beyond core Secure Service Edge (SSE) to better connect and protect your business

Features and Benefits

Table 1. Features and Benefits

Feature	Benefit
Zero Trust Network Access (ZTNA)	Provide granular, app-specific access to private applications in on-premises data centers or in cloud/IaaS environments. Based on defined access control policies, it uses least privilege principles and contextual insights to granularly deny access by default and brokers user access to applications when explicitly granted, irrespective of location. • Two access methods: Client-based and clientless browser-based access, granular user, and application-based access policy, SAML authentication, built-in Identity Provider (IdP), and contextual access control. • Client-based access leverages the unified Cisco Secure Client. • Establishes secure access after a device posture check is performed. • Authenticates users through a secure, encrypted tunnel, allowing users to see only applications and services they have permission to access. • Application proxy provides transparent, secure remote access without exposing the applications to the Internet. It even hides the network details of private apps from the clients accessing those apps. This prevents attackers from learning anything from IP reconnaissance even if they have compromised a client device, • Prevents lateral attacker movement. • Implement location and device-specific access control policies, preventing possibly compromised devices from connecting to its services. • Administrators 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. • Provides user with helpful information explaining the cause of denied access
VPNaaS	Not all private apps can be covered by ZTNA. VPNaaS cloud-based option is included for secure remote access as well as secure internet access for non-web internet traffic • Functionality examples include: Use case support (split tunneling and tunnel all support, peer-to-peer communication, trusted network detection, BYO certificate, split DNS, dynamic split DNS); multiple authentication methods (SAML, Certificate, Radius, LDAP); user ease of use (always on VPN, start before logon); IT operation simplification (Local IP Pool, multiple VPN profiles) • Enables remote users to access private applications via the Security Access fabric using the Cisco Secure Client. • Identity-based access control is available using SAML authentication through the customer's IdP. • Endpoint posture is also evaluated; this enables granular access control to private resources.
Secure Web Gateway (full proxy)	Log and inspect all web traffic over ports 80/443 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 all downloaded files for malware and other threats • Sandboxing with Cisco Secure Malware Analytics analyzes unknown files (see dedicated section for Cisco Secure Malware Analytics)

	• File type blocking (e.g., block download of .exe files) • Full or selective SSL decryption to protect from hidden attacks and time-consuming 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
Cloud access security broker (CASB)	Expose shadow IT by detecting and reporting on cloud applications in use. Manage cloud adoption, reduce risk, and block the use of offensive, non-productive, risky, or inappropriate cloud applications. • Data loss prevention (DLP) to prevent sensitive data exfiltration from leaving the organization and in the cloud (see separate DLP section) • 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 • Cloud malware detection to detect and remove malware from cloud-based file storage applications and ensure that data held withing the applications remain malware-free. • Ability to block/allow specific cloud applications • Tenant restrictions to control the instance(s) of SaaS applications that all users or specific groups/individuals can access
Data Loss Prevention (DLP)	Multimode data loss prevention. Analyze sensitive data in-line to provide visibility and control over sensitive data leaving your organization. API-based DLP functionality for out-of-band analysis of data at rest in the cloud. Includes unified policies and reporting. • 190+ built-in content classifiers including GDPR, PCI-DSS, HIPAA, PII, and PHI • Customizable built-in content classifiers with threshold and proximity to tune and reduce false positives • User-defined dictionaries with custom phrases (such as project code names) • Detection and reporting on sensitive data usage and drill-down reports to help identify misuse • Inspection of cloud app and web traffic content and enforcement of data policies
Firewall as a Service (FWaaS)	Provides visibility and control for non-web traffic that originated from requests going to the internet, across all ports and protocols. Includes mobile apps, peer-to-peer file sharing, collaboration (e.g. Webex or ZOOM), O365, or any non-web or non-DNS traffic. • Deployment, management and reporting through the Security Access single, unified dashboard • Customizable policies (IP, port, protocol, application and IPS policies) • Layer 3 / 4 firewall to log all activity and block unwanted traffic using IP, port, and protocol rules • Scalable cloud compute resources eliminate appliance capacity concerns • Layer 7 application visibility and control to Identify a growing base of over 2,800 non-web applications and selectively block or allow • Decrypts traffic prior to inspection.
Intrusion prevention system (IPS)	IPS examines network traffic flows and prevents vulnerability exploits with an added layer of threat prevention using SNORT 3 technology and signature-based detection. • Using a unified dashboard, create policies to examine traffic and take automated actions to catch and drop dangerous packets before they reach the network. • Provides IPS protection for both internet and private traffic. • Configure access-policies and options for different custom profiles depending on traffic destination.

	• Uses an extensive and growing base of over 40,000 signatures from Cisco Talos • Signatures are available in pre-defined templates, which are customizable. • Detection and blocking of vulnerability exploitation.
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, track file execution actions, and capture network activity generated by the file. When combined with Investigate, 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 • Single, correlated source of intelligence to speed threat hunting and incident response • APIs to integrate with XDR and commonly used SIEMs for enriching security data • Retrospective notification if file disposition changes (originally good / later deemed malicious)
Remote Browser Isolation (RBI)	RBI protects users and organizations from browser-based threats. It shifts the execution of browsing activity from the user to a remote cloud-based virtualized browser instance to protect from Internet threats. Website code is run separately and only a safe visual stream is delivered to the user. This is fully transparent to the end user. No need to worry about malware that hasn't been detected yet. • 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	Enforces filtering at the DNS layer to block requests to malicious and unwanted destinations before a connection is established. Blocks threats over any port or protocol before they reach the network or endpoints. • Protects internet access across all network devices, office locations, and roaming users • Provides detailed reporting for DNS activity by type of security threat or web content and the action taken • Retains logs of all activity • Accelerated rollout to thousands of locations and users to provide immediate protection
Talos threat intelligence	Talos, a leading provider of cutting-edge security research globally, analyses 100s of billions of DNS requests and other telemetry data daily. It continuously runs AI, statistical, and machine learning models against this massive database to provide insight into cyber threats and improve incident response rates. • Uncover malicious domains, IPs, malware, and URLs before they're used in attacks. • Prioritize incident investigations • Speed incident investigations and response • Predict future attack origins by pinpointing and mapping out attackers' infrastructures

Cloud malware detection	Detects and removes malware from cloud-based file storage applications. 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, and Microsoft 365.
Single management and reporting console	Unified security policy creation, including intent-based rules, and management across internet, public SaaS apps, and private app access. Provides extensive logging and the ability to export logs to enterprise SOC, etc. • 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 org. • Unified source (users, devices) and unified resources (apps, destination) ensures that the security policy follows the users no matter the point of attach and no matter which app is accessed. • Reduces on-going policy management activities. • Improves visibility and time-to-detection with aggregated reporting. • Simplifies the overall SOC/security analyst investigation process.
App Connectors	App Connectors simplify administrative tasks to setup secure connectivity to private applications. They connect Cisco Secure Access to customer data centers. • Reduce SSE team's dependency on network teams for devices 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.

Packaging options

Cisco Secure Access is the broadest SSE solution and is available in a single subscription to drive better security outcomes and improved productivity. It 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 Access Essentials and Cisco Secure Access Advantage.

Table 2. Core Offer Package

Category	Features	Secure Access Essentials	Secure Access Advantage
Secure Access	Secure internet access • Roaming Security • SD-WAN DIA integration • VPNaaS	✓	✓
	Secure private access • Client-based ZTNA • Clientless ZTNA • VPNaaS	✓	✓
Foundational Security	Cloud Delivered Firewall for layer 3 & layer 4 controls of web and private apps	✓	✓
	Secure web gateway (proxy web traffic, URL filtering, content filtering, advanced app controls)	✓	✓
	CASB - Cloud app discovery, risk scoring, blocking, cloud malware detection; tenant controls	✓	✓
	Remote Browser Isolation (Risky*)	✓	✓
	Secure Malware Analytics (sandbox)	Limited	Unlimited
Advanced Security	Layer 7 Cloud Delivered Firewall		✓
	IPS protection		✓
	Data Loss Prevention (DLP) for web applications		✓
	Remote Browser Isolation (All**)		✓
Support	Cisco 24x7 enhanced support access via email and phone	✓	✓

*Risky: Isolate uncategorized websites and security categories (including potentially harmful)

**All: Isolate any chosen destination, including content and security categories, destination lists, applications, uncategorized, etc.

For more information

For more information, please visit: Cisco Secure Access.

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**.

05/23