Cisco Secure Access for Government

Protect the mission with cloud-agile security

June 2025

Contents

Hybrid work and security service edge

Today's hybrid work environments require a revised approach to security. Security Service Edge (SSE) is a key enabler of any organization's hybrid-work and cloud 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 can enjoy a secure, transparent user experience, anywhere they work – office, home, or on the road. For the highest effectiveness, SSE solutions must deliver superior user experience – enhancing productivity, reducing IT complexity, and improving security efficacy.

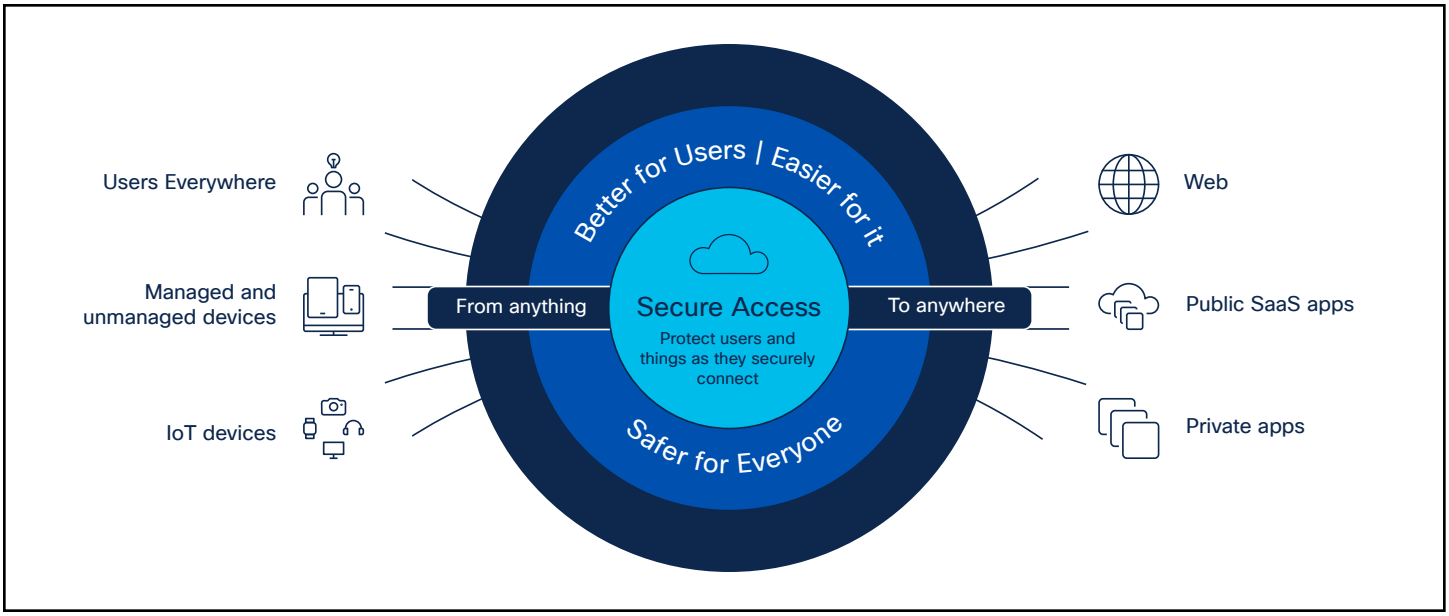

Figure 1. Secure connectivity from anything to anywhere

Cisco Secure Access for Government product overview

Cisco Secure Access for Government is a cloud-delivered SSE solution, grounded in zero trust, that provides seamless, transparent, and secure user access from managed and unmanaged devices to any type of application (internet, SaaS, private) whether hosted in the cloud or on-premises. It includes SSE components (ZTNA, SWG, CASB, and FWaaS) plus extended capabilities including VPN-as-a-Service (VPNaaS), integrated inline and SaaS API-based DLP, Talos Threat Intelligence, RBI, DNS, Protective DNS (CISA) Security, and much more—in one license and management platform. Agencies can now protect users as they seamlessly access 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, and more. It integrates with other Cisco offerings including Duo and Catalyst SD-WAN. Secure Access adapts security to reduce risk, simplifies IT operations to lower complexity, and provides users with efficient, frictionless access to raise productivity.

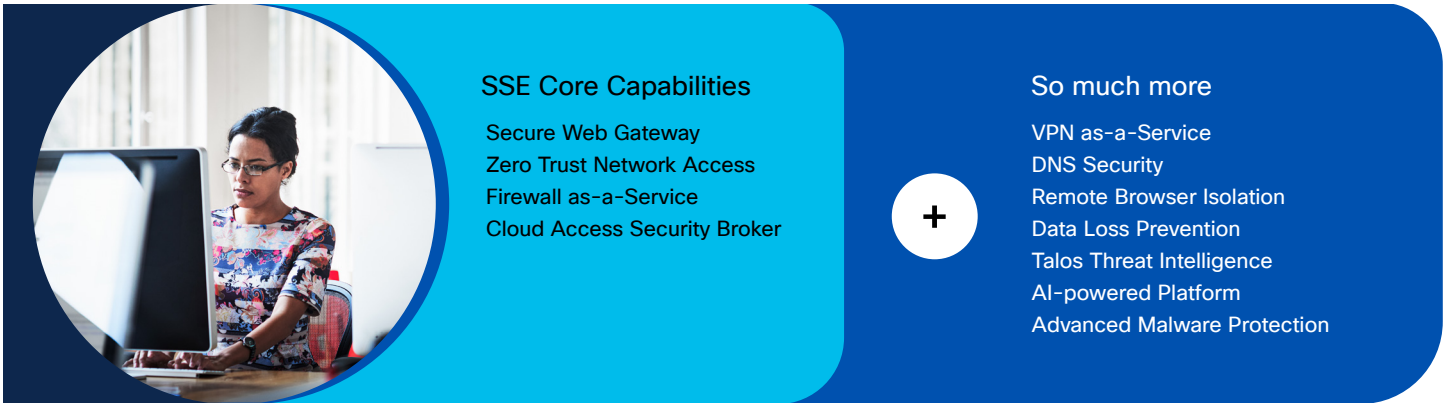

Figure 2. Cisco Secure Access for Government capabilities

Increase human effectiveness with security that is better for users

By improving the user experience, Secure Access for Government may not only increase user productivity but may also remove the temptation to try to circumvent security procedures which can increase risk. A single, unified client simplifies how users connect; they can authenticate and go straight to the desired app.

For private app access, users automatically and transparently connect via ZTNA or VPNaaS, without needing unnecessary extra steps or repeating cumbersome verification tasks. Cisco's high-performance architecture uses MASQUE and QUIC protocols and is built on Vector Packet Processing (VPP) to speed connections and lower latency. This minimizes hassles for the users, and can significantly increases productivity, while enhancing security.

Simplified operations makes it easier for IT

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

Cisco Secure Access simplifies and automates operations via a single, cloud-managed console with 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, apps, and devices. IT may do less manual aggregation as it rapidly detects and blocks threats, expedites investigations, and minimizes remediation tasks, while deepening visibility into end-user activity.

Adaptive security that's safer for everyone

The Cisco Secure Access zero-trust architectural approach, which aims to secure against sophisticated cyber threats, has been acknowledged for industry-leading security efficacy. End-users can be 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 can block unsanctioned app usage. Cloaking internal resources and preventing hackers from discovering their presence generates an extra layer of security to protect the mission.

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, governments can maintain mission continuity and may decrease the risk of a breach.

A part of Cisco's Single-Vendor SASE Solution

Secure Access for Government can be combined with Cisco's FedRAMP authorized SD-WAN solutions to create a unique, single-vendor SASE experience for government agencies and their contractors. Seeking simplicity, security, and performance? Look no further. By delivering an integrated platform that eliminates the challenges of multivendor management, Cisco will empower organizations to cost-effectively manage secure access, increase application performance and availability, and establish continuous visibility. This enables users and IT teams to focus on their mission while maintaining robust security and connectivity through a modern architecture.

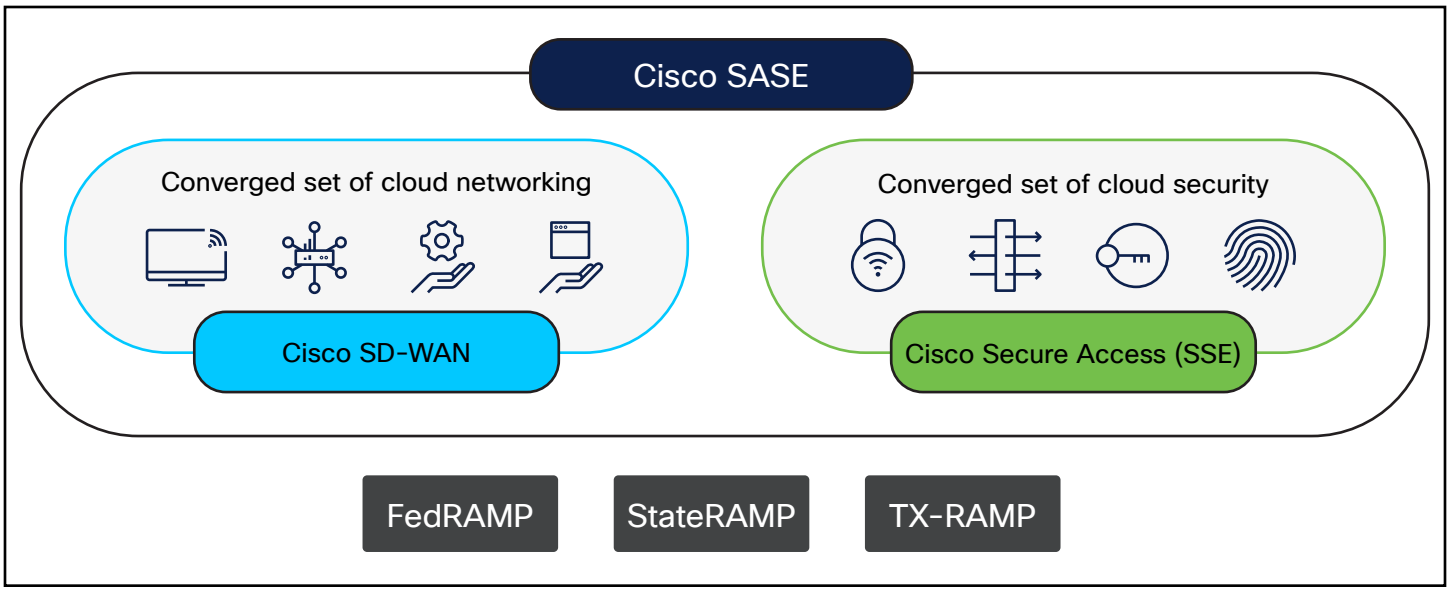

Figure 3. Cisco Single-Vendor SASE FedRAMP authorized solution

Compliance

Strengthening cyber resilience with zero trust and SSE

Federal and SLED organizations face constant pressure from a broad spectrum of threats—ransomware, phishing, data breaches, and insider attacks. Addressing these risks starts with a zero trust approach: strict identity verification, granular access controls, and continuous monitoring of user and device behavior.

Zero trust is designed to ensure access is only granted to those who need it—and nothing more. It is also designed to create a foundation for detecting suspicious activity early, reducing the blast radius of any potential breach.

Tackling compliance with confidence

Meeting regulatory requirements is not optional—it's a foundational part of cybersecurity for government and public sector organizations.

Cisco Secure Access for Government supports your compliance strategy with built-in capabilities designed to align to federal and state mandates. Through its zero trust and secure service edge (SSE) architecture, Secure Access for Government helps agencies meet complex requirements while securing users, data, and applications across distributed and hybrid environments.

Key compliance challenges Cisco helps address:

- **Regulatory complexity:** Navigating overlapping federal and state security mandates can drain time and IT resources.
- **Distributed workforce:** Remote and field-based employees create a wide attack surface that must remain compliant and protected.
- **Hybrid infrastructure:** Security must remain consistent across on-prem and cloud-based systems as agencies modernize their environments.

Cisco Secure Access is **FedRAMP moderate authorized** and supports leading government frameworks, including.

- **NIST 800-53**
- **TIC 3.0**
- **Executive Order 14028**

Built for trust—built for you

Cisco Secure Access for Government is designed to help agencies comply with today's security mandates and adapt to what's next.

Its zero trust architecture operates on a "never trust, always verify" model. Every access request is treated as though it comes from an untrusted source. Every user, device, and application is authenticated and continuously verified.

SSE enhances this by bringing core security functions—like secure web gateway, cloud firewall, and DNS-layer protection—into a unified, cloud-delivered platform. This ensures agencies can maintain visibility and control without adding needless complexity.

Together, zero trust and SSE help you:

- Gain consistent protection across environments
- Minimize lateral movement
- Reduce risk and simplify security operations

Mission-focused. Compliance-ready

For over 40 years, Cisco has helped government agencies build secure, resilient infrastructure. Cisco Secure Access for Government continues that tradition with a cloud-first, compliance-aware solution that protects sensitive data and supports evolving mission needs.

Whether you're aligning with federal frameworks or managing distributed teams, Cisco helps you build with confidence—knowing compliance, security, and performance are built in from day one.

See additional compliance information for Secure Access.

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/IaaS environments. 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 through the Cisco Secure Client, the single, unified client for Secure Access. • Clientless access (through a browser) protects traffic to web apps (http/https). • 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). • 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; creating posture profiles that evaluate diverse endpoints and browsers; enforcing additional user authentication for specific apps; and much more.
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, 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, 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.
	• More than 1200 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.
	• **AI Access feature set** (phased implementation for FedRAMP, expected to begin phasing in AI features in June 2025):
	  – Enables visibility and control of over 1200 LLMs to control Shadow AI usage;
	  – For ChatGPT and other LLMs, control or block ingress and egress of source code via Web and API interfaces.
	  – Machine learning-based DLP uses pre-training to identify and protect documents like patent applications, nondisclosure agreements, merger and acquisition related content, 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.
	• API-based content inspection functionality supports Microsoft 365 (SharePoint and OneDrive), Google Drive, Webex, Box, Dropbox, Slack, ServiceNow.

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
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.
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.

Feature	Benefit
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.
Protective DNS integration (PDNS)	Secure Access for Government provides an integration with CISA's Protective DNS which enables compliance with this mandate plus the enhanced policies, analytics and control of Cisco DNS-layer security. This integration was developed in partnership with CISA so it meets their requirements. • Enables the power of Cisco DNS-layer security and forwards DNS traffic to CISA as required by law. • Provides detailed analytics, and real time detection and protection. • Integrated with other Cisco features like profiles and policies. • Easy-to-configure integration through the Admin interface.
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 through 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 ongoing 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 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. SWG protection for the Chrome browser. • Next generation mobile device support for Apple and Samsung (see section below on mobile device ZTNA support).

Packaging options

Cisco Secure Access for Government 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.

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 www.cisco.com/go/secure-access-gov.

C78-5177225-00 06/25