Cisco Secure Access for Government

Cisco's FedRAMP-Moderate authorized Security Service Edge (SSE) solution is built to meet government advanced security requirements, increase operational efficiency, and secure high-performance teams.

Why it matters

Government agencies face mounting pressure to protect sensitive data, support flexible work environments, and modernize IT—all while remaining compliant and efficient. Fragmented tools and outdated architectures increase risk and create friction for both users and IT teams. Cisco Secure Access for Government addresses these challenges by unifying key security functions into a single, cloud-centered, intelligent platform.

At a glance

In today's distributed government environment, security must extend beyond traditional perimeters—protecting users, data, and applications across devices, locations, and clouds. Cisco Secure Access for Government delivers a unified Secure Service Edge (SSE) platform that empowers agencies to protect the workforce from risks, reduce IT complexity, and accelerate mission outcomes—all while designed to maintain compliance with federal and state mandates.

Built on zero trust principles and powered by Cisco Talos's unmatched intelligence, Cisco Secure Access for Government combines adaptive security, seamless access, and operational simplicity in a cloud-native, FedRAMP-authorized solution.

Three key benefits of Cisco Secure Access for Government

1. Adaptive security that's safer for everyone

Proactively defend the number one attack target—your workforce—with intelligence-driven protection that evolves with the threat landscape.

- **Real-time detection and prevention:** AI and ML-powered analytics, backed by Cisco Talos, which analyzes over 800 billion signals daily to detect threats before they disrupt operations.
- **Seamless cloud-native enforcement:** Apply consistent protection for internet and private app access through integrated ZTNA, SWG, CASB, DLP, FWaaS, and VPNaaS.
- **DNS-layer defense:** Stop threats across any port or protocol with differentiated recursive DNS protection, implemented with CISA's Protective DNS guidance.
- **Enables U.S. Federal** Government agencies to meet requirements of OMB Mandate M22-09 (zero trust), CISA Protective DNS, and Enhanced Cybersecurity, with FedRAMP-Moderate authorization, StateRAMP, and TX-RAMP. Meets FIP2, standards for 140-2 encryption, NIST 800-53 rev 5, and TIC 3.0.

Unlike fragmented solutions...

Cisco Secure Access for Government offers a converged platform that combines all major SSE functions, unified client access, and threat intelligence from Talos in one solution. It reduces tool sprawl, improves threat visibility, and helps provide consistent, policy-driven protection from the data center to the cloud to the edge.

2. Increase human effectiveness with security that’s better for users

Enable your workforce to do their best work without compromising security or user experience.

- **Unified client access:** The industry’s first client to combine ZTNA and VPN, delivering secure, reliable access to every type of application, over any protocol.
- **Modern, high-speed connectivity:** MASQUE and QUIC protocols create isolated, tunnel-less sessions for each app—improving performance and reducing attack surfaces.
- **Frictionless experience:** Transparent, behind-the-scenes protection keeps users productive without unnecessary prompts or slowdowns.
- **Granular access control:** Define access by user role, ensuring appropriate access to critical resources while blocking unauthorized attempts.

3. Operational simplicity makes it easier for IT

Streamline IT management while improving performance, reducing costs, and increasing control.

- **Single console and policy engine:** Centralized visibility and enforcement help reduce administrative overhead and policy gaps.
- **AI-optimized protection:** Talos machine learning optimizes threat detection, helping IT teams respond faster.
- **Built for compliance:** Integrates with FedRAMP Moderate-authorized solutions such as Duo and Cisco Catalyst SD-WAN to support zero-trust architectures.
- **Scalable, resilient architecture:** Built on Cisco’s high-performance platform using Vector Packet Processing (VPP), delivering up to 8 times the throughput of other SSE solutions.

A part of Cisco's single-vendor SASE solution

Secure Access for Government can be combined with Cisco's FedRAMP-authorized Catalyst 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 empowers 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.

Proven, trusted, ready

Cisco Security Service Edge solutions are trusted by more than 30,000 organizations worldwide. Whether your agency is a supporting a workforce in the office or remotely, transitioning to the cloud, or aligning with zero trust and other security frameworks like NIST, CISA, TIC 3.0, and more, Cisco provides the unified security foundation needed to protect national interests and maintain public trust.

Learn more

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

Contact your Cisco account representative to schedule a demo or discuss a custom deployment strategy for your agency.